Today's Ethernet

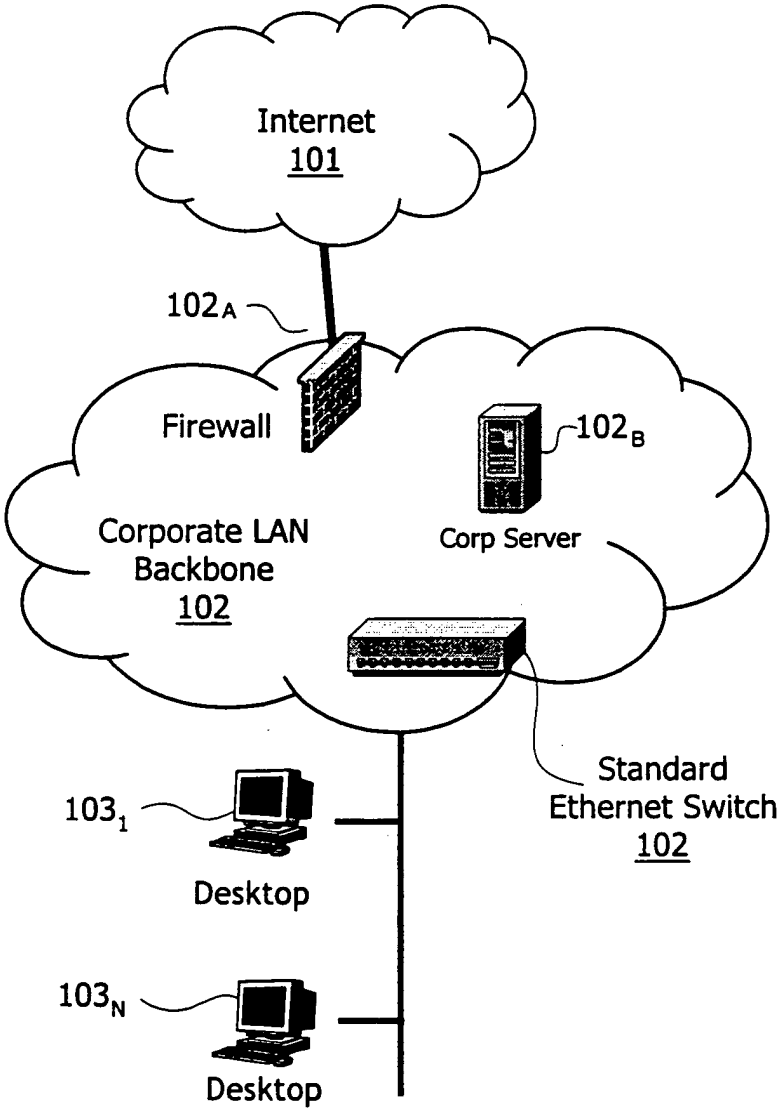


FIG. 1

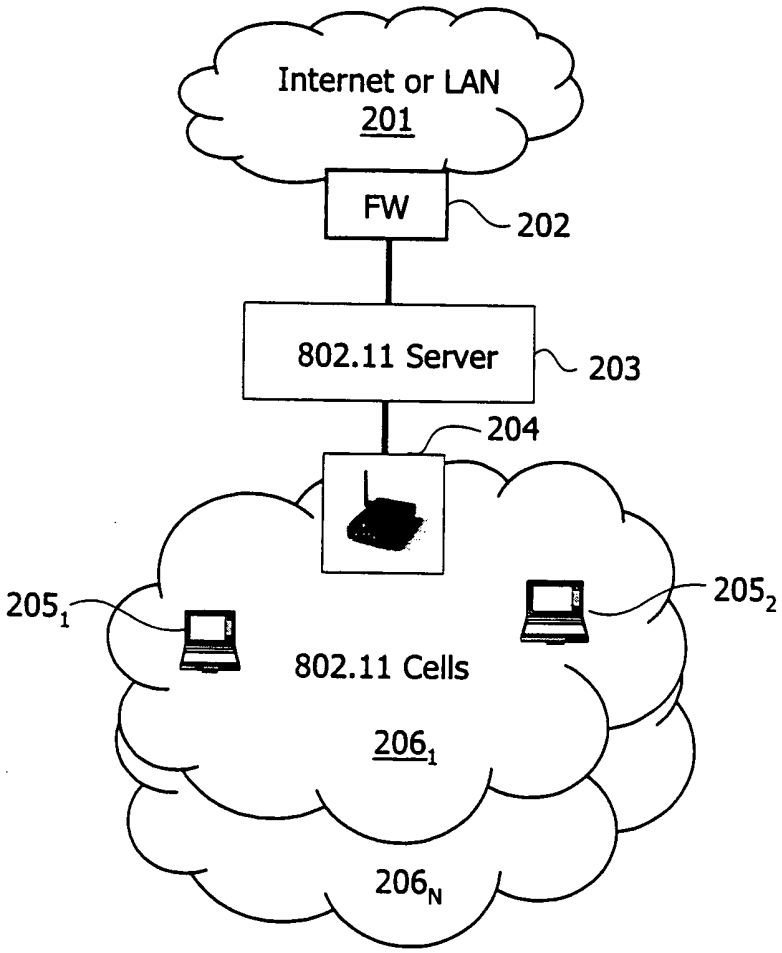

Internet or LAN
201
FW
202
802.11 Server
203
204
205$_1$
205$_2$
802.11 Cells
206$_1$
206$_N$

FIG. 2

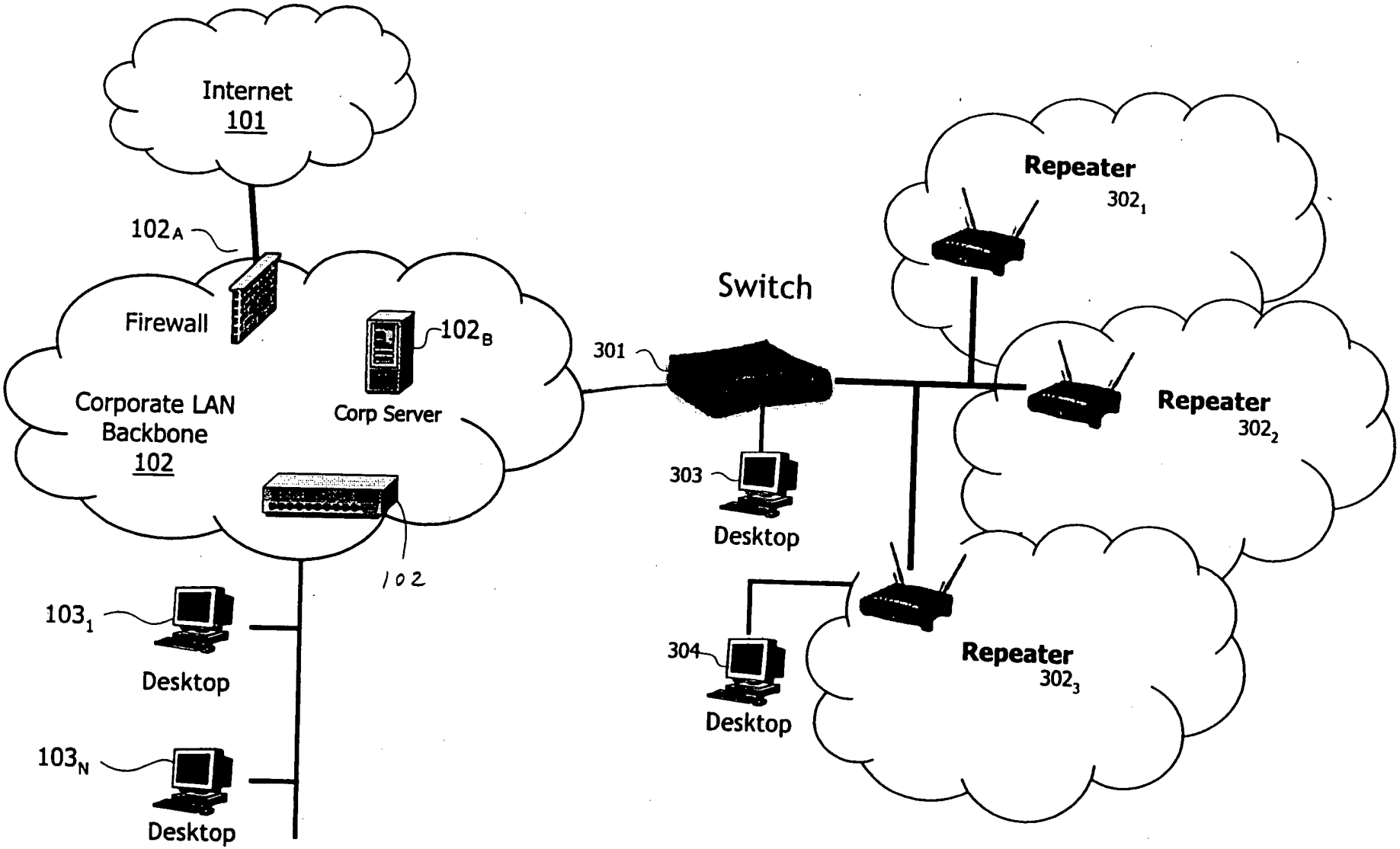

Internet
101
102A
Firewall
102B
Corp Server
Corporate LAN
Backbone
102
102
Switch
301
303
Desktop
Repeater
3021
Repeater
3022
Repeater
3023
304
Desktop
1031
Desktop
103N
Desktop

FIG. 3

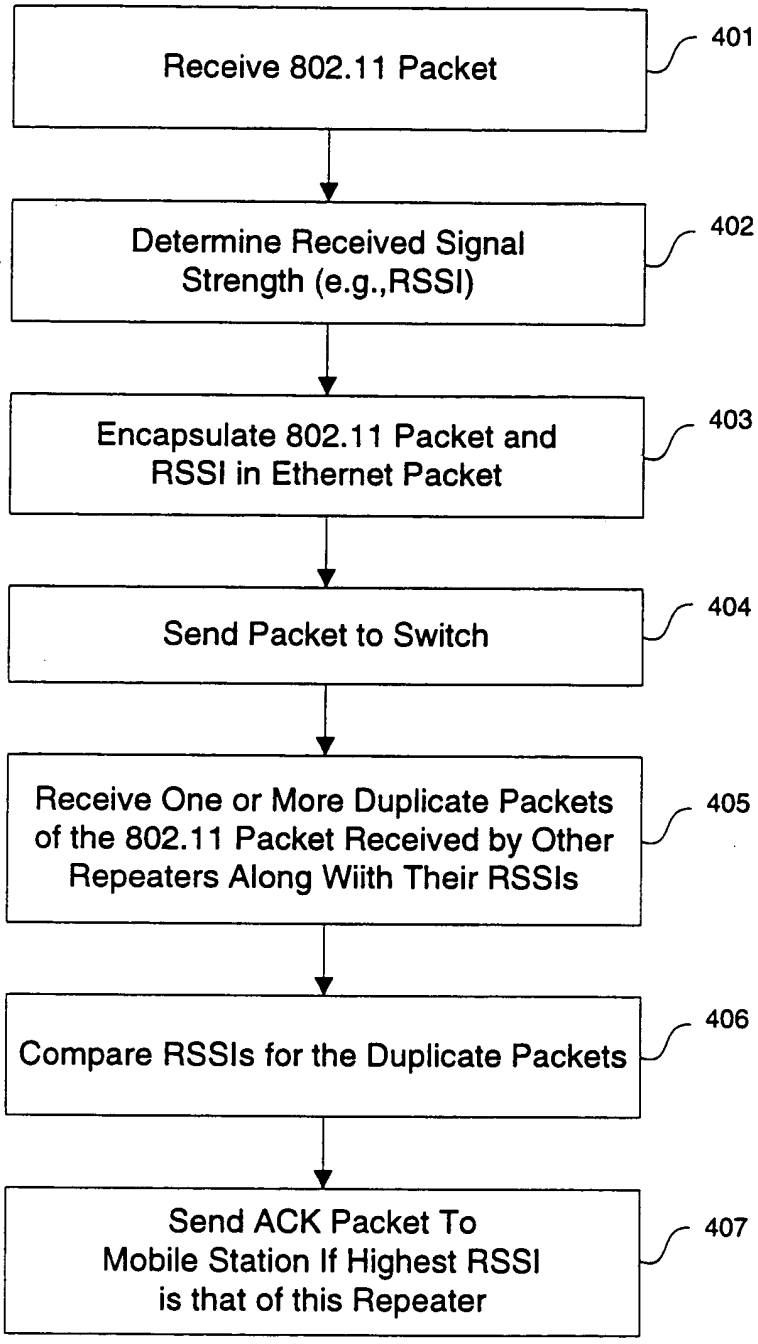

Receive 802.11 Packet
401
Determine Received Signal Strength (e.g.,RSSI)
402
Encapsulate 802.11 Packet and RSSI in Ethernet Packet
403
Send Packet to Switch
404
Receive One or More Duplicate Packets of the 802.11 Packet Received by Other Repeaters Along Wiith Their RSSIs
405
Compare RSSIs for the Duplicate Packets
406
Send ACK Packet To Mobile Station If Highest RSSI is that of this Repeater
407

FIG. 4A

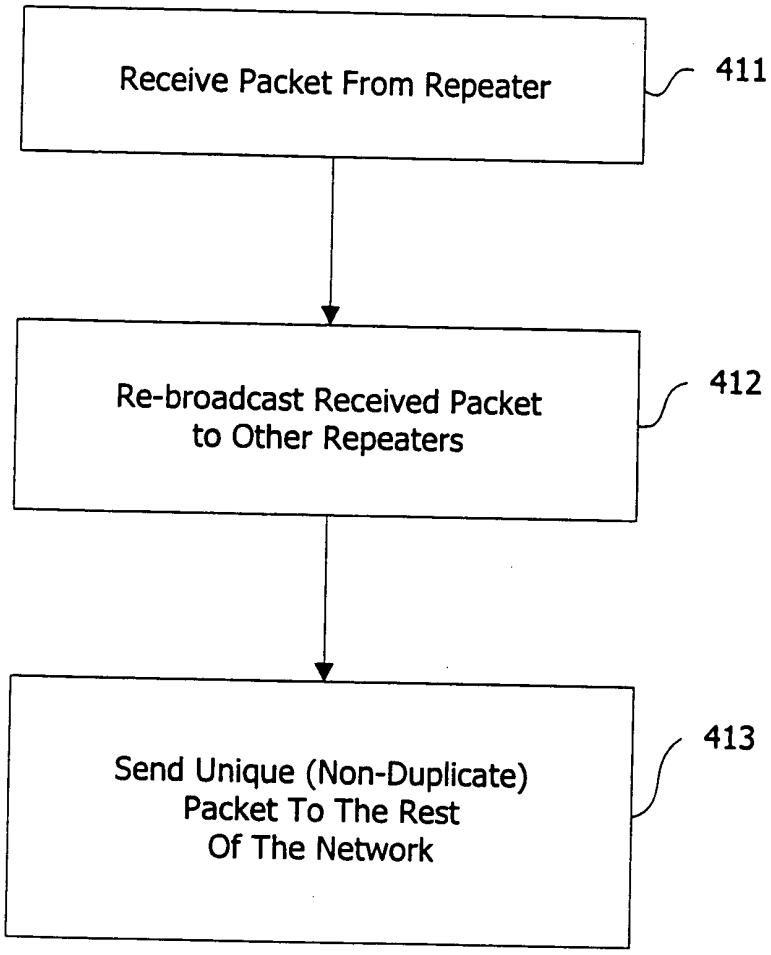

Receive Packet From Repeater
411
Re-broadcast Received Packet to Other Repeaters
412
Send Unique (Non-Duplicate) Packet To The Rest Of The Network
413

FIG. 4B

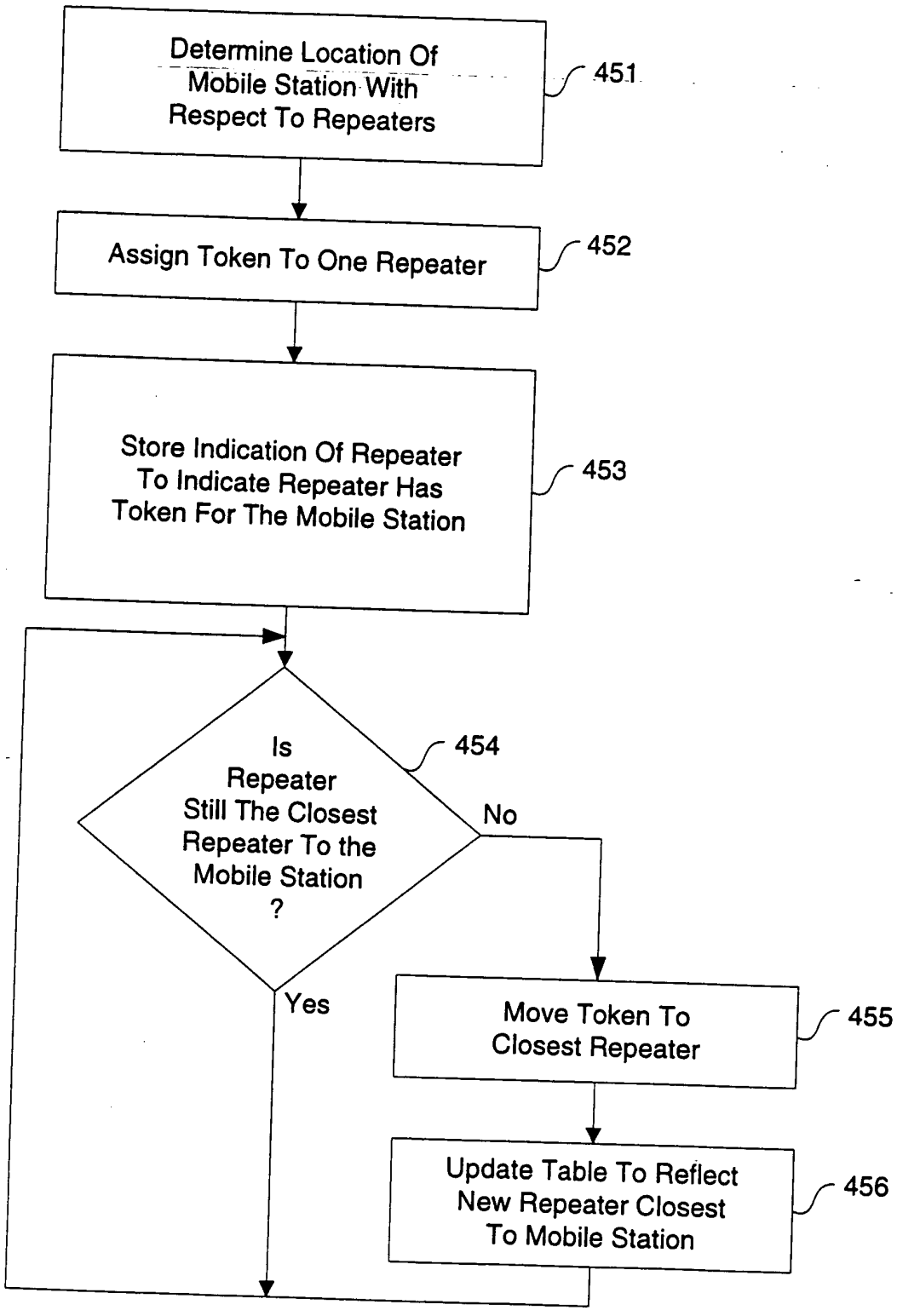

Determine Location Of Mobile Station With Respect To Repeaters
451
Assign Token To One Repeater
452
Store Indication Of Repeater To Indicate Repeater Has Token For The Mobile Station
453
Is Repeater Still The Closest Repeater To the Mobile Station ?
454
No
Yes
Move Token To Closest Repeater
455
Update Table To Reflect New Repeater Closest To Mobile Station
456

FIG. 4C

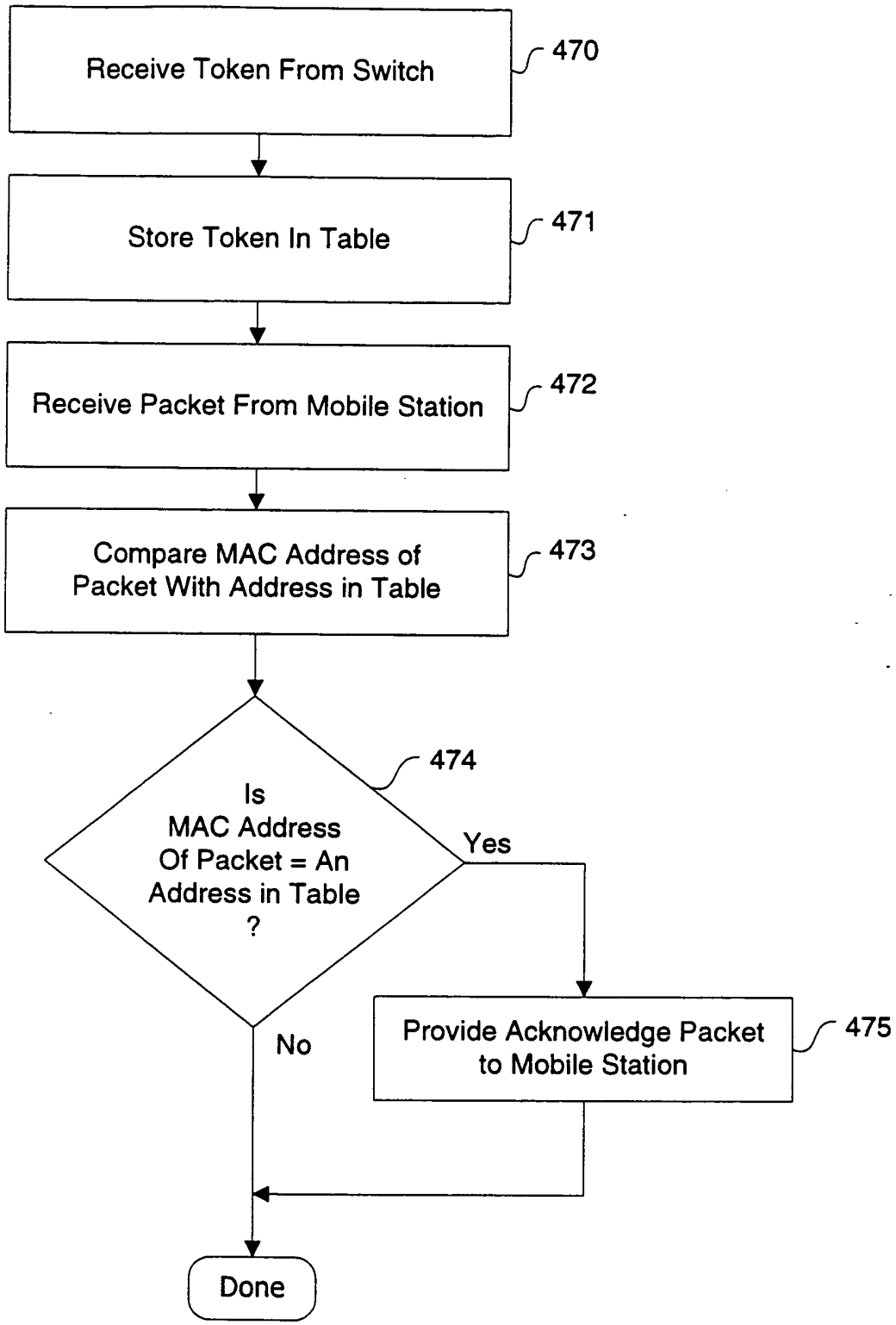

Receive Token From Switch
470
Store Token In Table
471
Receive Packet From Mobile Station
472
Compare MAC Address of Packet With Address in Table
473
Is MAC Address Of Packet = An Address in Table ?
474
Yes
No
Provide Acknowledge Packet to Mobile Station
475
Done

FIG. 4D

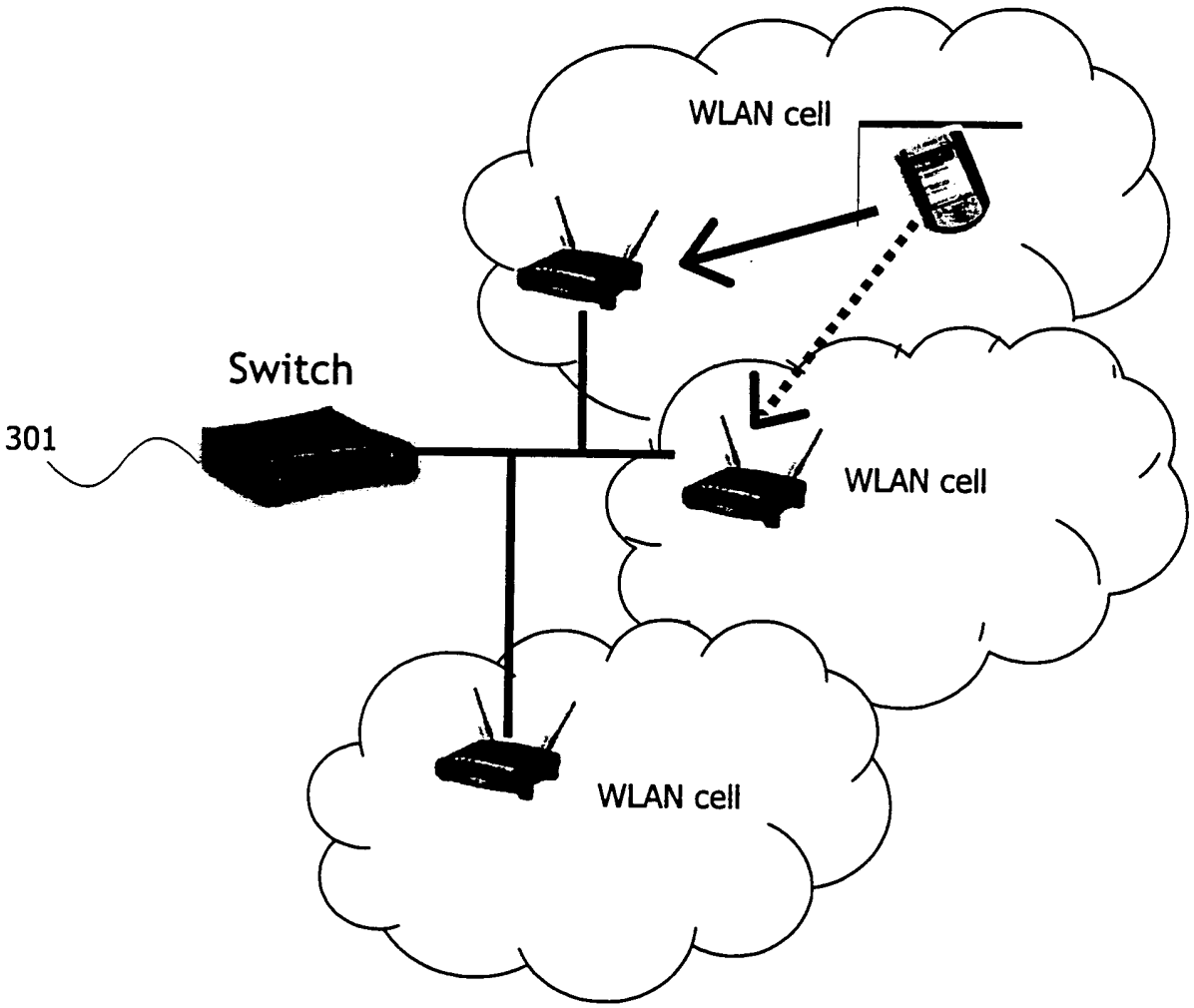


FIG. 5A

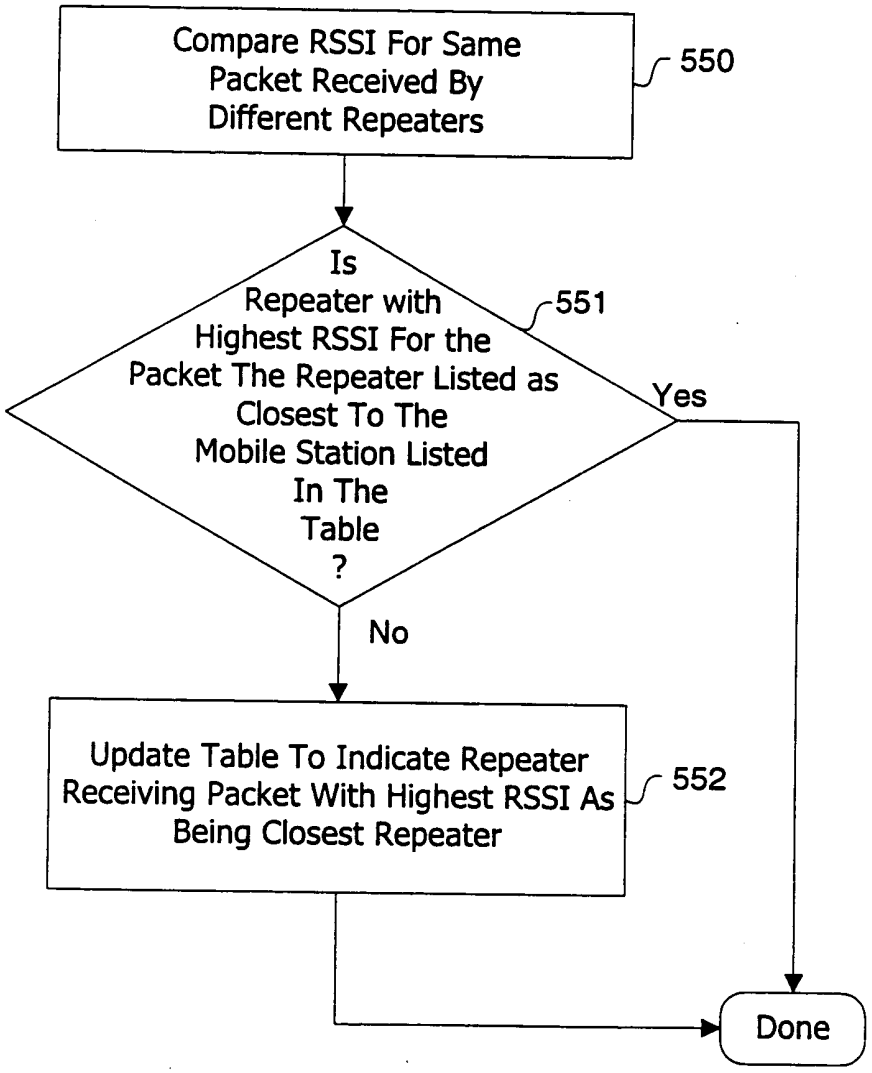

Compare RSSI For Same Packet Received By Different Repeaters
550
Is Repeater with Highest RSSI For the Packet The Repeater Listed as Closest To The Mobile Station Listed In The Table ?
551
Yes
No
Update Table To Indicate Repeater Receiving Packet With Highest RSSI As Being Closest Repeater
552
Done

FIG. 5B

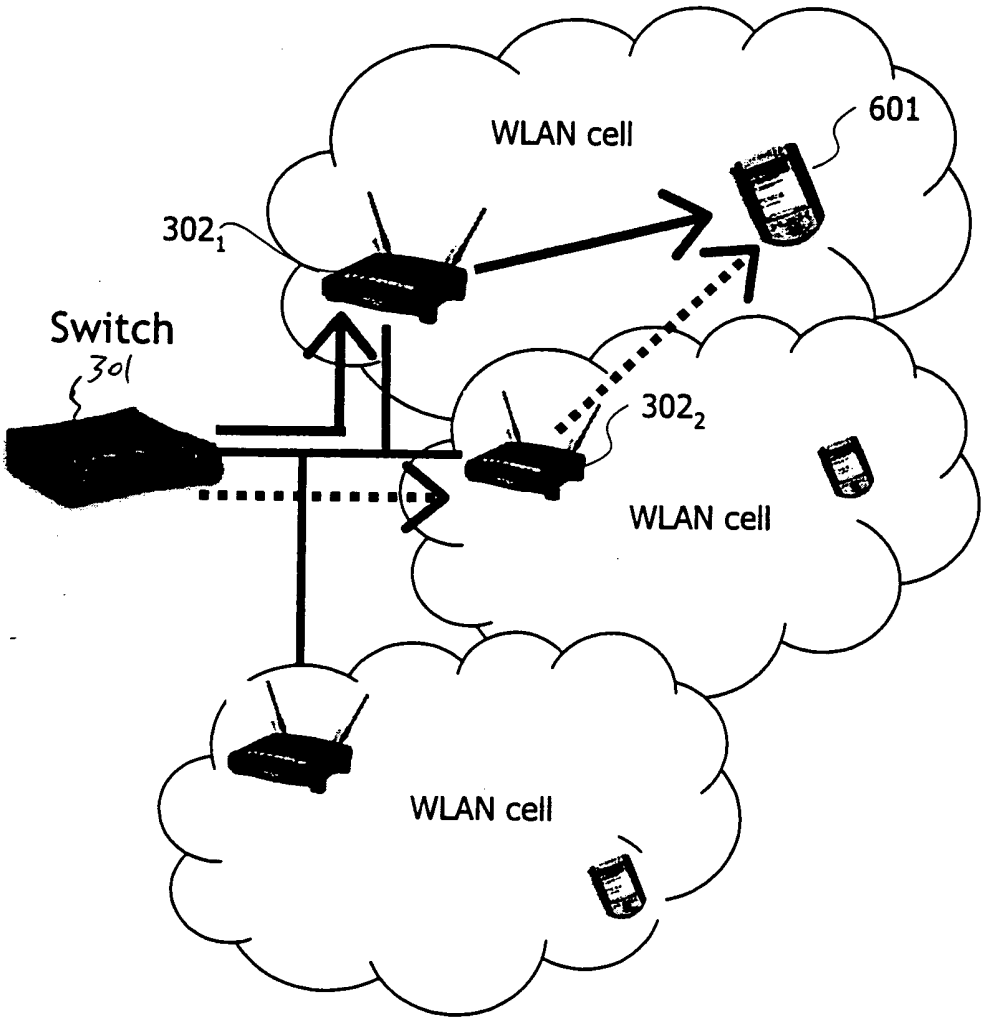


FIG. 6

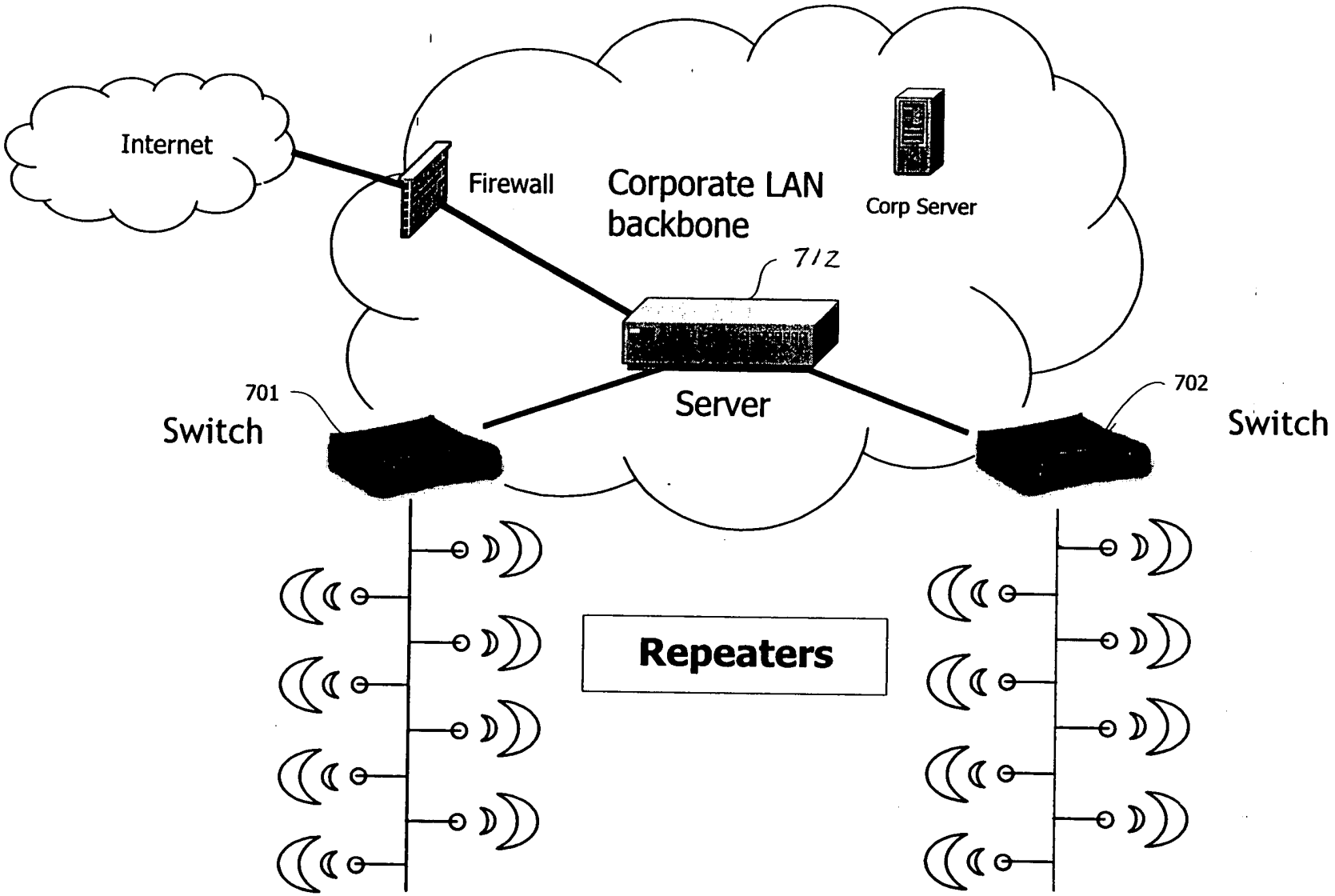

Internet
Firewall
Corporate LAN backbone
Corp Server
712
Server
701
Switch
702
Switch
Repeaters

FIG. 7

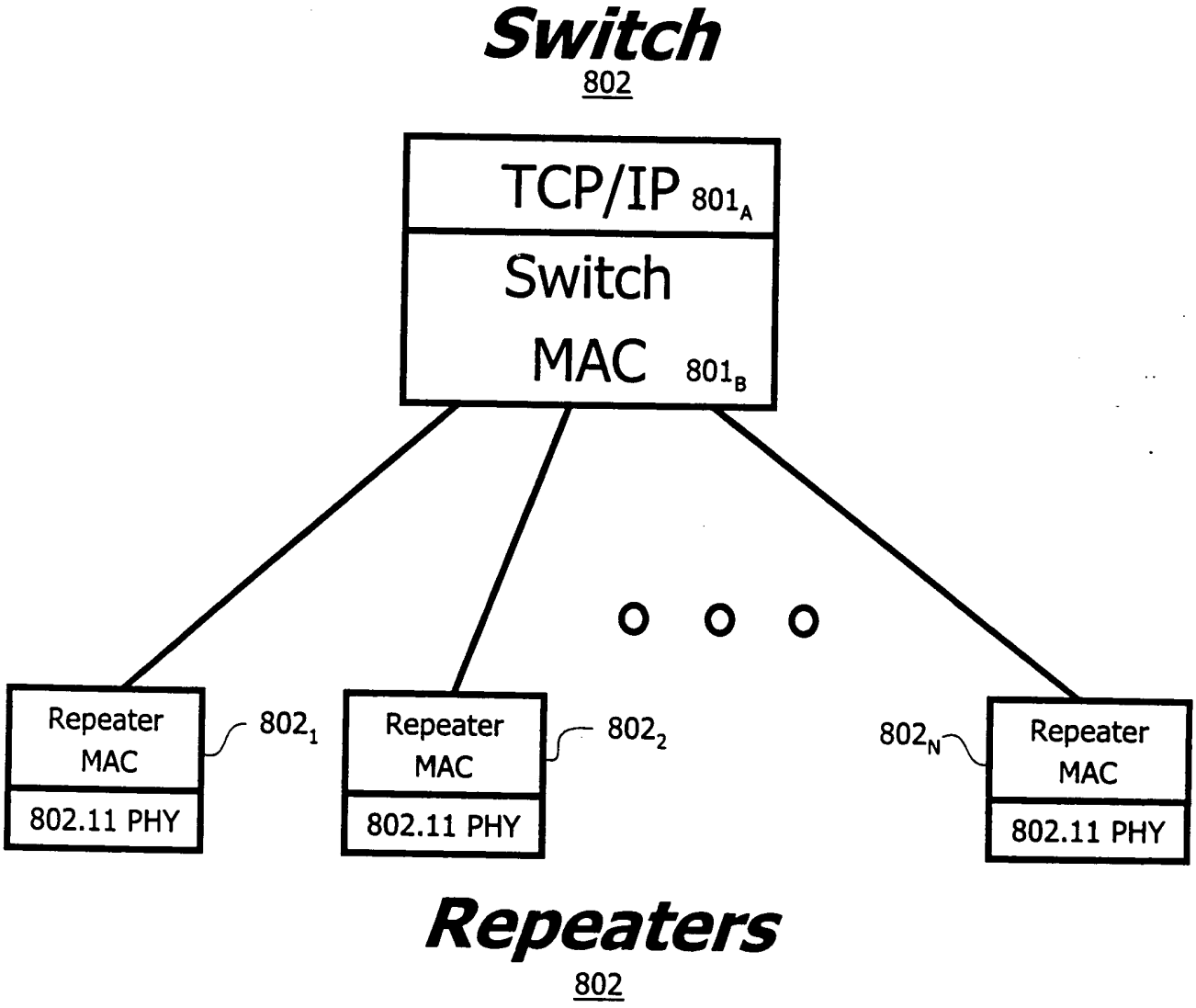

Switch
802
TCP/IP 801A
Switch MAC 801B
Repeater MAC
802.11 PHY
802.1
Repeater MAC
802.11 PHY
802.2
802N
Repeater MAC
802.11 PHY
Repeaters
802

FIG. 8

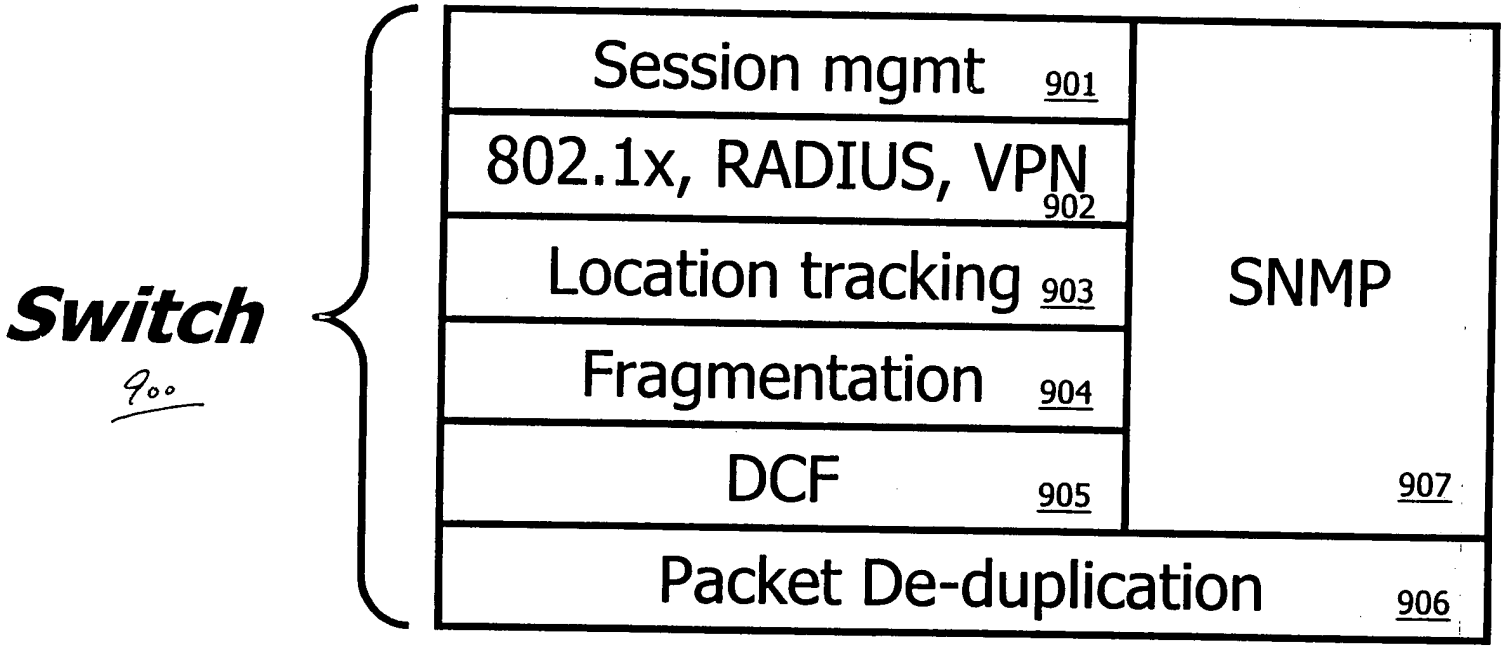

Switch
900
Session mgmt 901
802.1x, RADIUS, VPN 902
Location tracking 903
Fragmentation 904
DCF 905
Packet De-duplication 906
SNMP 907

FIG. 9A

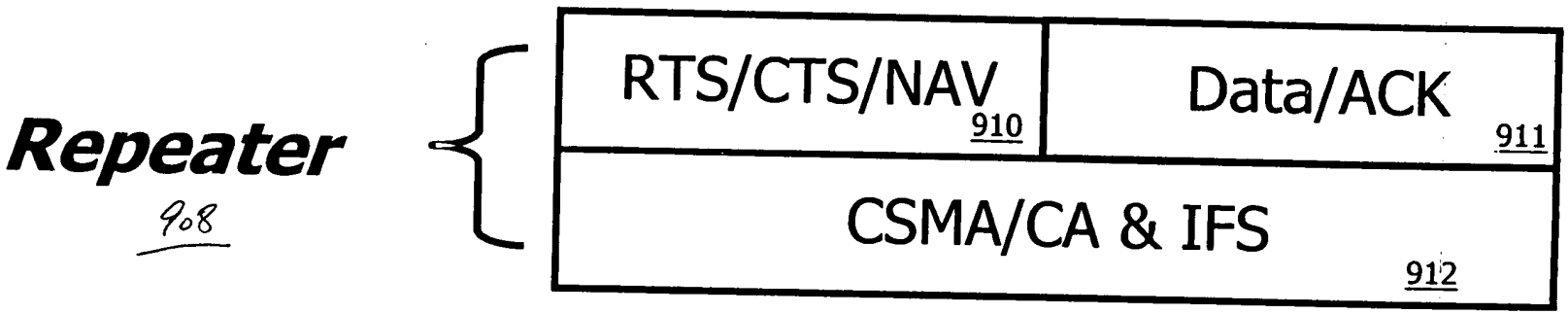


FIG. 9B

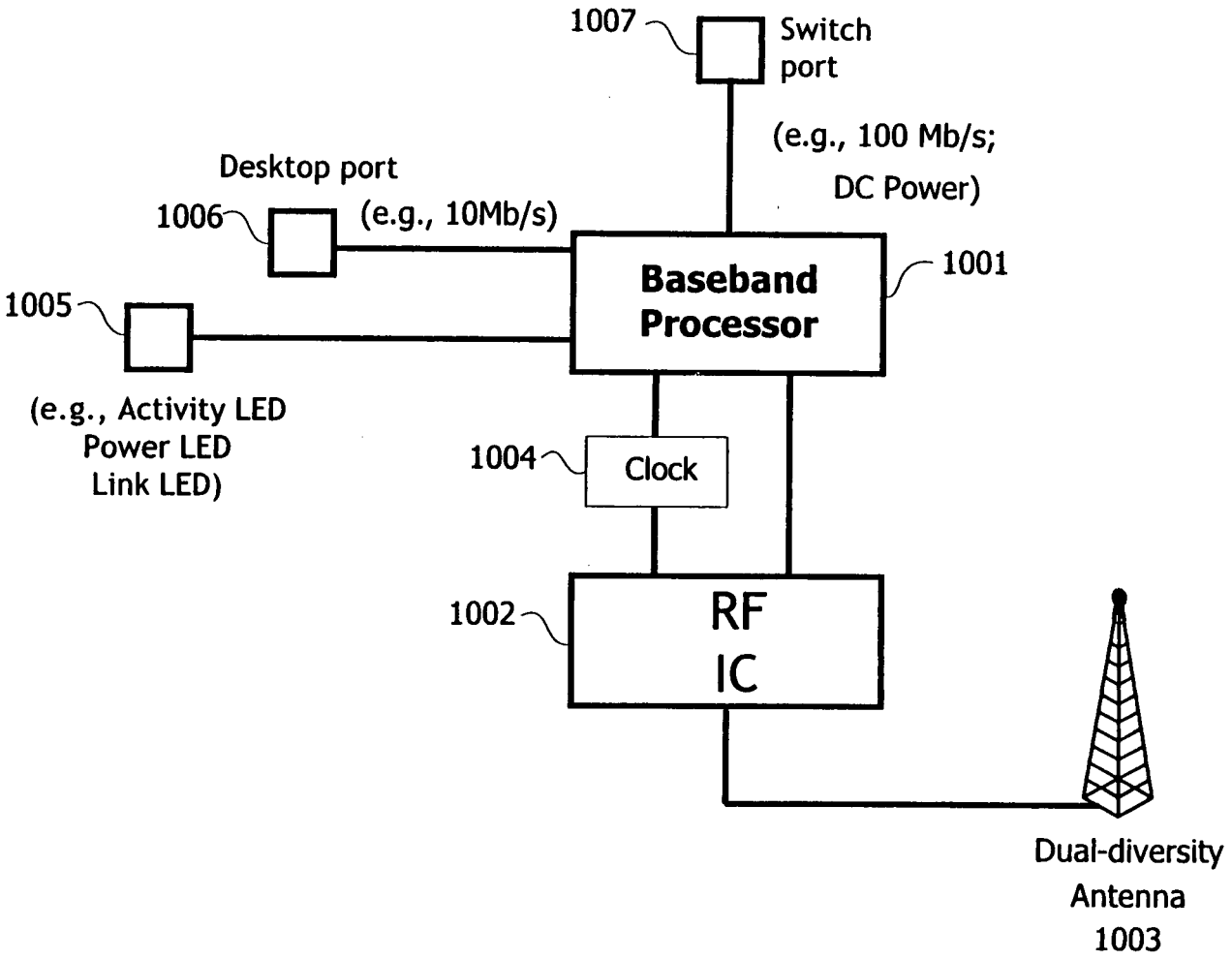

1007
Switch port
(e.g., 100 Mb/s; DC Power)
Desktop port
1006
(e.g., 10Mb/s)
1001
Baseband Processor
1005
(e.g., Activity LED
Power LED
Link LED)
1004
Clock
1002
RF IC
Dual-diversity Antenna 1003

FIG. 10

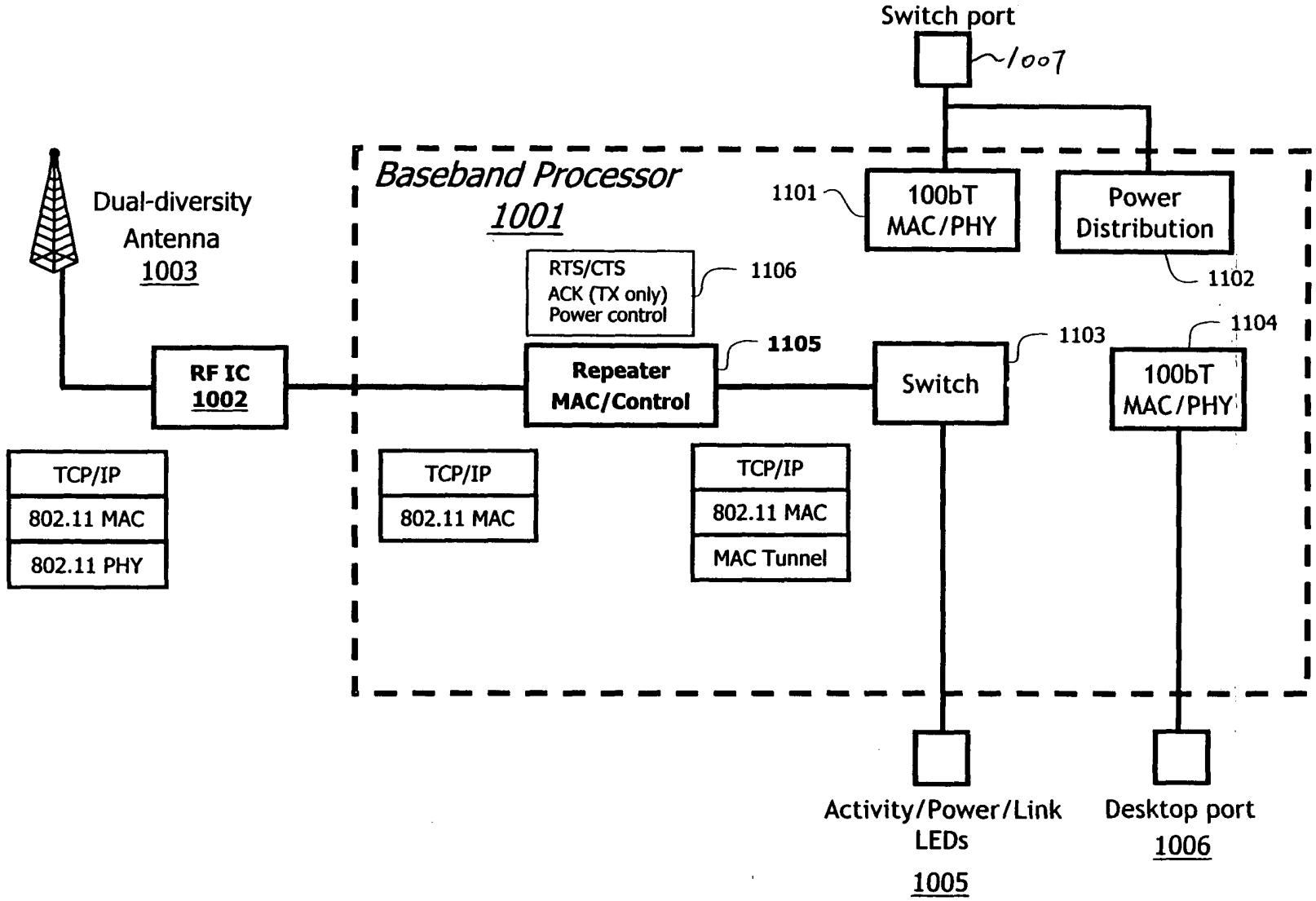

Switch port
1007
Baseband Processor
1001
1101
100bT
MAC/PHY
Power
Distribution
1102
RTS/CTS
ACK (TX only)
Power control
1106
1105
1103
1104
Dual-diversity
Antenna
1003
RF IC
1002
Repeater
MAC/Control
Switch
100bT
MAC/PHY
TCP/IP
802.11 MAC
802.11 PHY
TCP/IP
802.11 MAC
TCP/IP
802.11 MAC
MAC Tunnel
Activity/Power/Link
LEDs
1005
Desktop port
1006

FIG. 11

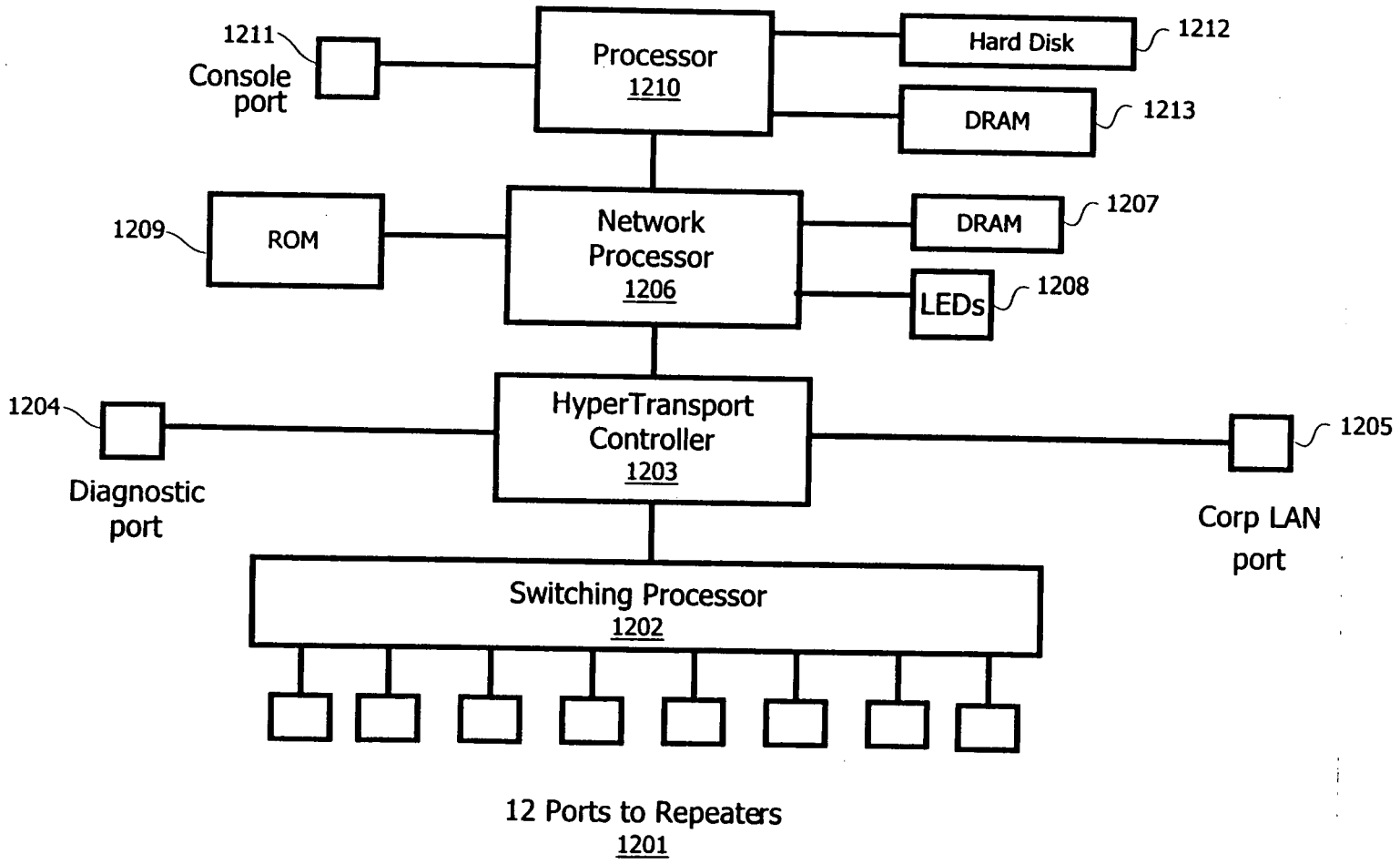

1211
Console port
Processor
1210
Hard Disk
1212
DRAM
1213
1209
ROM
Network Processor
1206
DRAM
1207
LEDs
1208
1204
Diagnostic port
HyperTransport Controller
1203
1205
Corp LAN port
Switching Processor
1202
12 Ports to Repeaters
1201

FIG. 12A

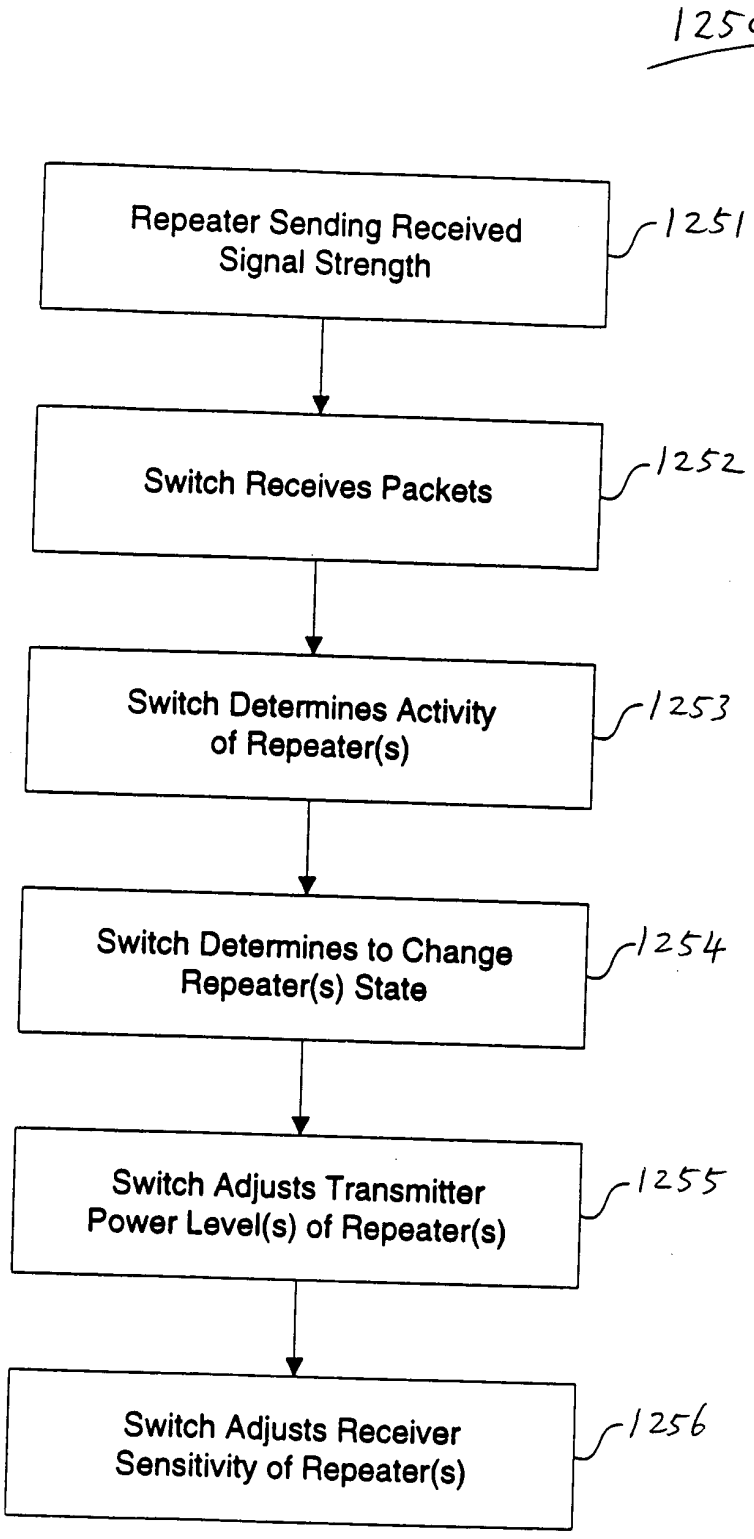

1250
Repeater Sending Received Signal Strength
1251
Switch Receives Packets
1252
Switch Determines Activity of Repeater(s)
1253
Switch Determines to Change Repeater(s) State
1254
Switch Adjusts Transmitter Power Level(s) of Repeater(s)
1255
Switch Adjusts Receiver Sensitivity of Repeater(s)
1256

Fig. 12B

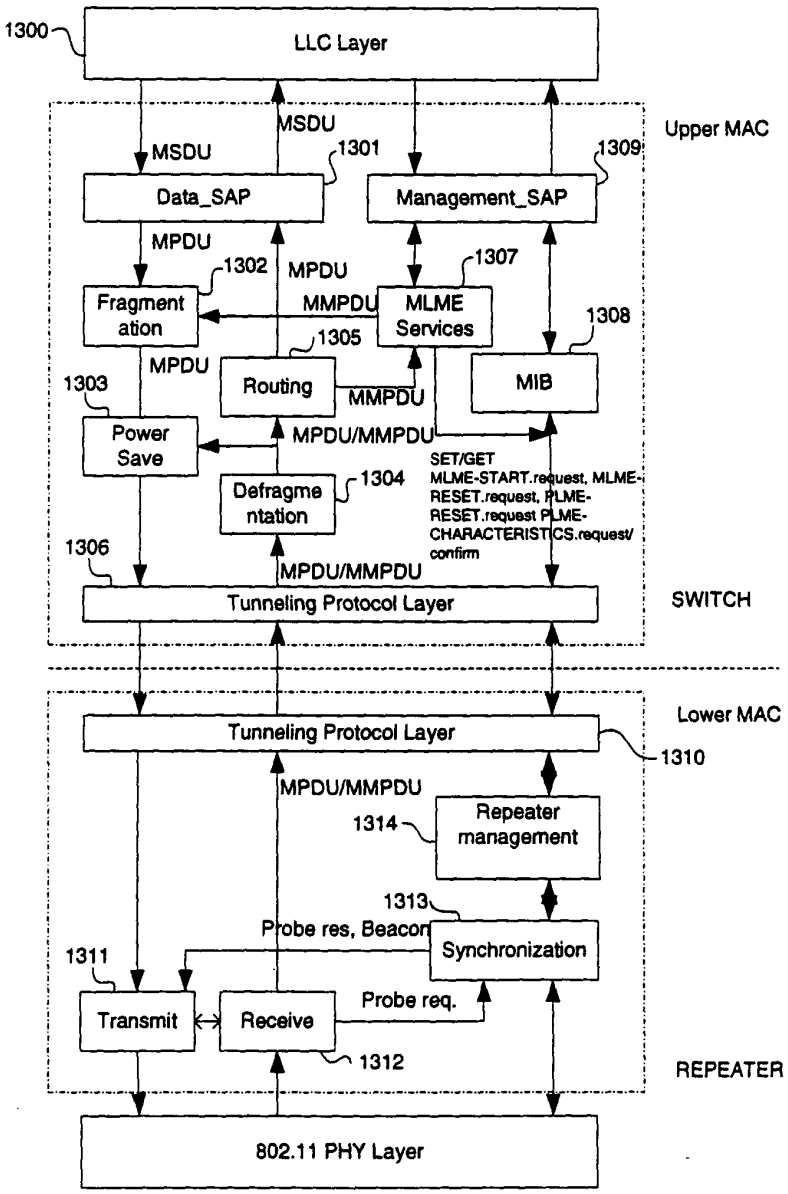
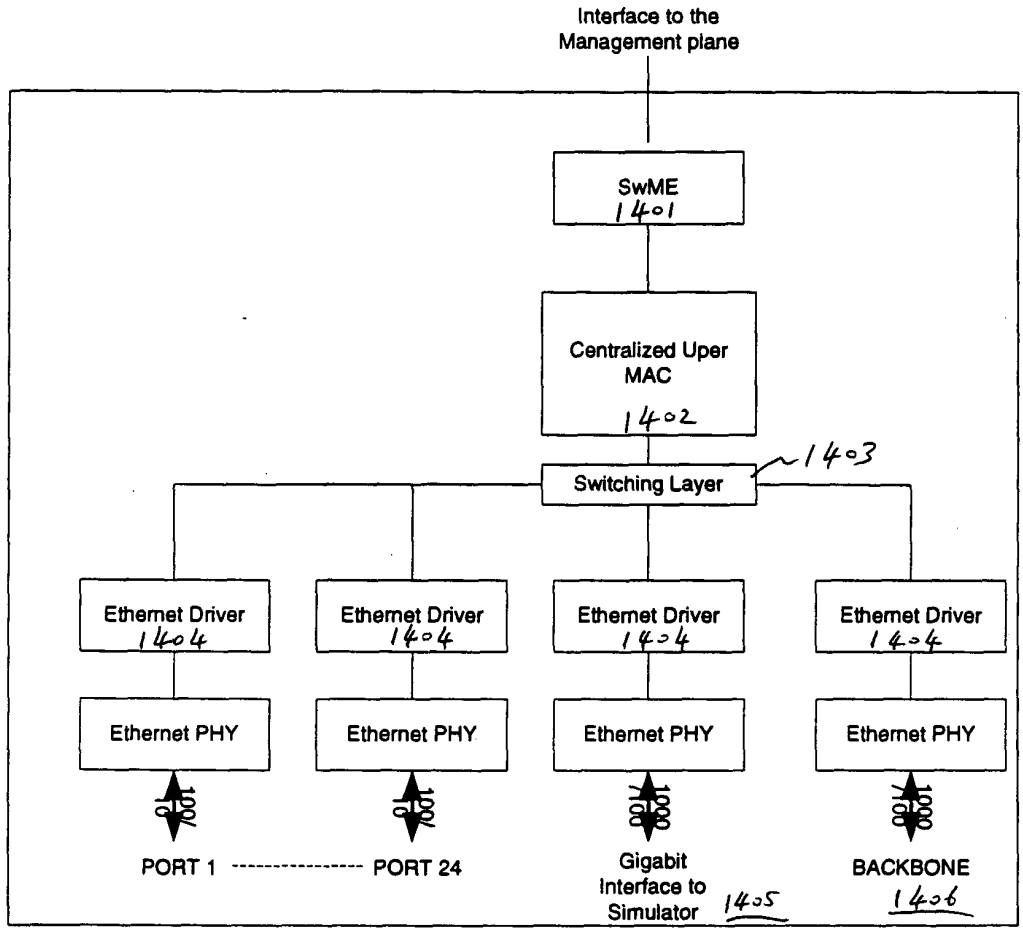

1300
LLC Layer
Upper MAC
MSDU
MSDU
1301
1309
Data_SAP
Management_SAP
MPDU
1302
MPDU
1307
Fragment ation
MMPDU
MLME Services
1308
1305
MPDU
1303
Routing
MMPDU
MIB
Power Save
MPDU/MMPDU
SET/GET MLME-START.request, MLME-RESET.request, PLME-RESET.request PLME-CHARACTERISTICS.request/ confirm
1304
Defragme ntation
1306
MPDU/MMPDU
Tunneling Protocol Layer
SWITCH
Lower MAC
Tunneling Protocol Layer
1310
MPDU/MMPDU
1314
Repeater management
1313
Probe res, Beacon
Synchronization
1311
Transmit
Receive
Probe req.
1312
REPEATER
802.11 PHY Layer

FIG. 13



SWITCHING PLANE 1400

FIG. 14

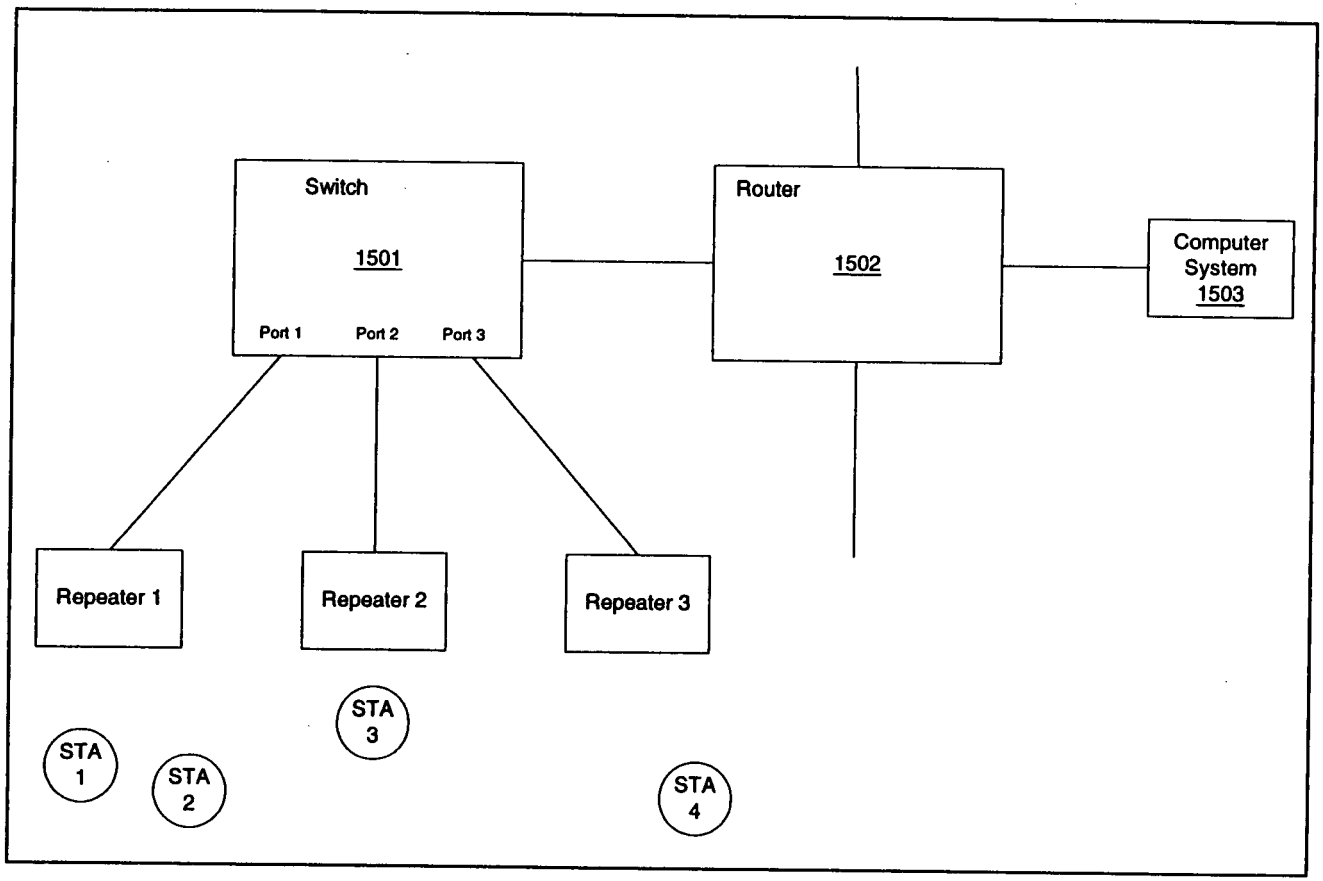

Switch
1501
Port 1
Port 2
Port 3
Router
1502
Computer System
1503
Repeater 1
Repeater 2
Repeater 3
STA 1
STA 2
STA 3
STA 4

FIG. 15

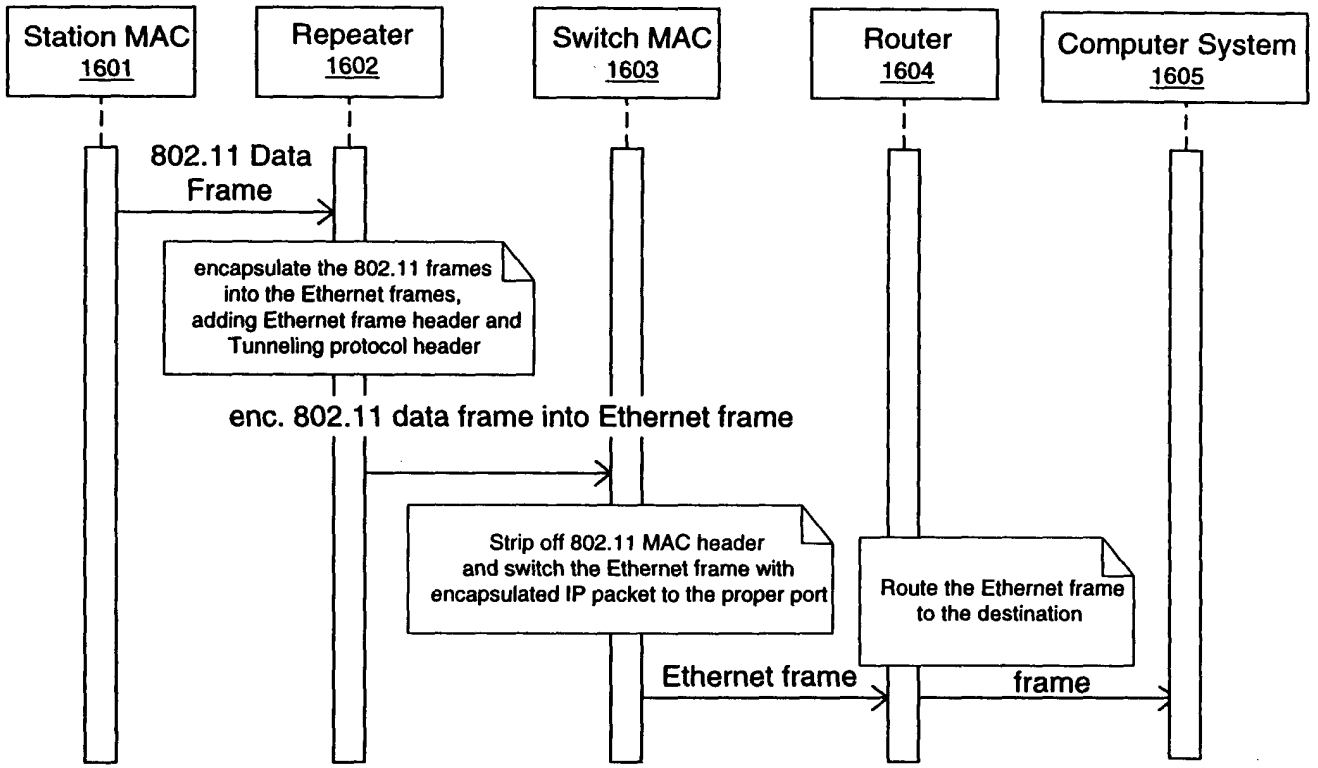

Station MAC
1601
Repeater
1602
Switch MAC
1603
Router
1604
Computer System
1605
802.11 Data Frame
encapsulate the 802.11 frames into the Ethernet frames, adding Ethernet frame header and Tunneling protocol header
enc. 802.11 data frame into Ethernet frame
Strip off 802.11 MAC header and switch the Ethernet frame with encapsulated IP packet to the proper port
Route the Ethernet frame to the destination
Ethernet frame
frame

FIG. 16

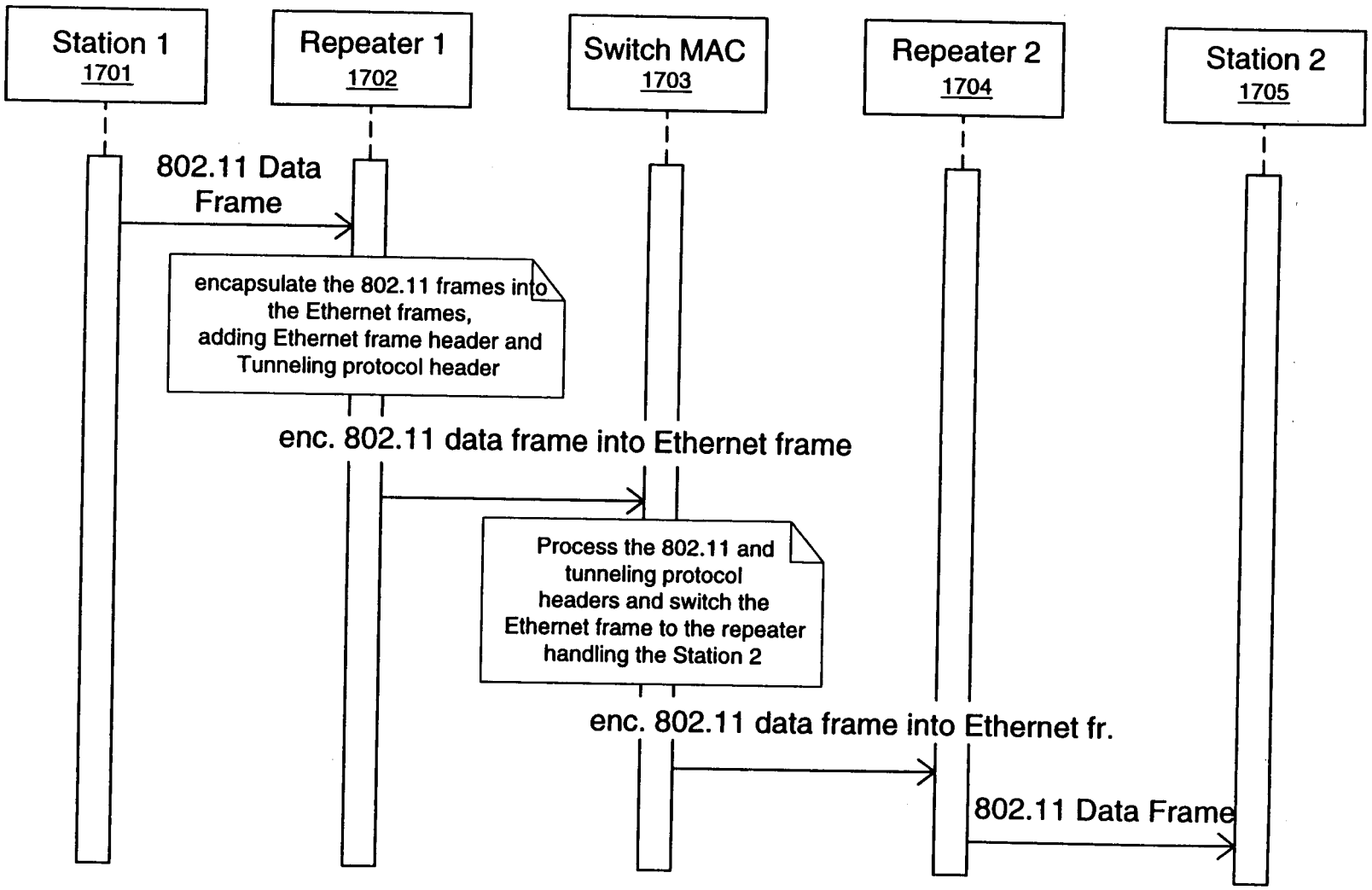

Station 1
1701
Repeater 1
1702
Switch MAC
1703
Repeater 2
1704
Station 2
1705
802.11 Data Frame
encapsulate the 802.11 frames into the Ethernet frames, adding Ethernet frame header and Tunneling protocol header
enc. 802.11 data frame into Ethernet frame
Process the 802.11 and tunneling protocol headers and switch the Ethernet frame to the repeater handling the Station 2
enc. 802.11 data frame into Ethernet fr.
802.11 Data Frame

FIG. 17.

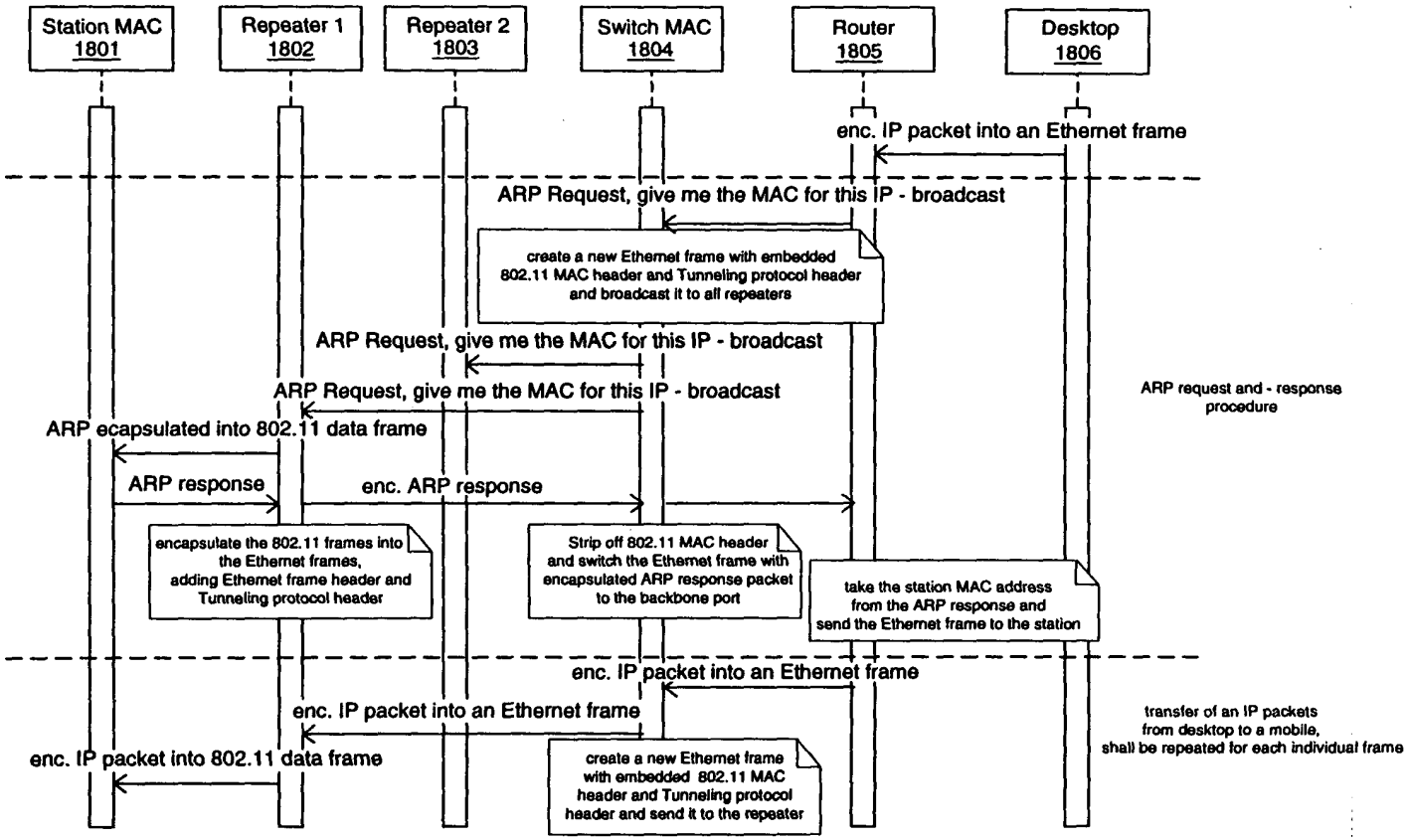

Station MAC
1801
Repeater 1
1802
Repeater 2
1803
Switch MAC
1804
Router
1805
Desktop
1806
enc. IP packet into an Ethernet frame
ARP Request, give me the MAC for this IP - broadcast
create a new Ethernet frame with embedded 802.11 MAC header and Tunneling protocol header and broadcast it to all repeaters
ARP Request, give me the MAC for this IP - broadcast
ARP Request, give me the MAC for this IP - broadcast
ARP ecapsulated into 802.11 data frame
ARP request and - response procedure
ARP response
enc. ARP response
encapsulate the 802.11 frames into the Ethernet frames, adding Ethernet frame header and Tunneling protocol header
Strip off 802.11 MAC header and switch the Ethernet frame with encapsulated ARP response packet to the backbone port
take the station MAC address from the ARP response and send the Ethernet frame to the station
enc. IP packet into an Ethernet frame
enc. IP packet into an Ethernet frame
transfer of an IP packets from desktop to a mobile, shall be repeated for each individual frame
enc. IP packet into 802.11 data frame
create a new Ethernet frame with embedded 802.11 MAC header and Tunneling protocol header and send it to the repeater

FIG. 18

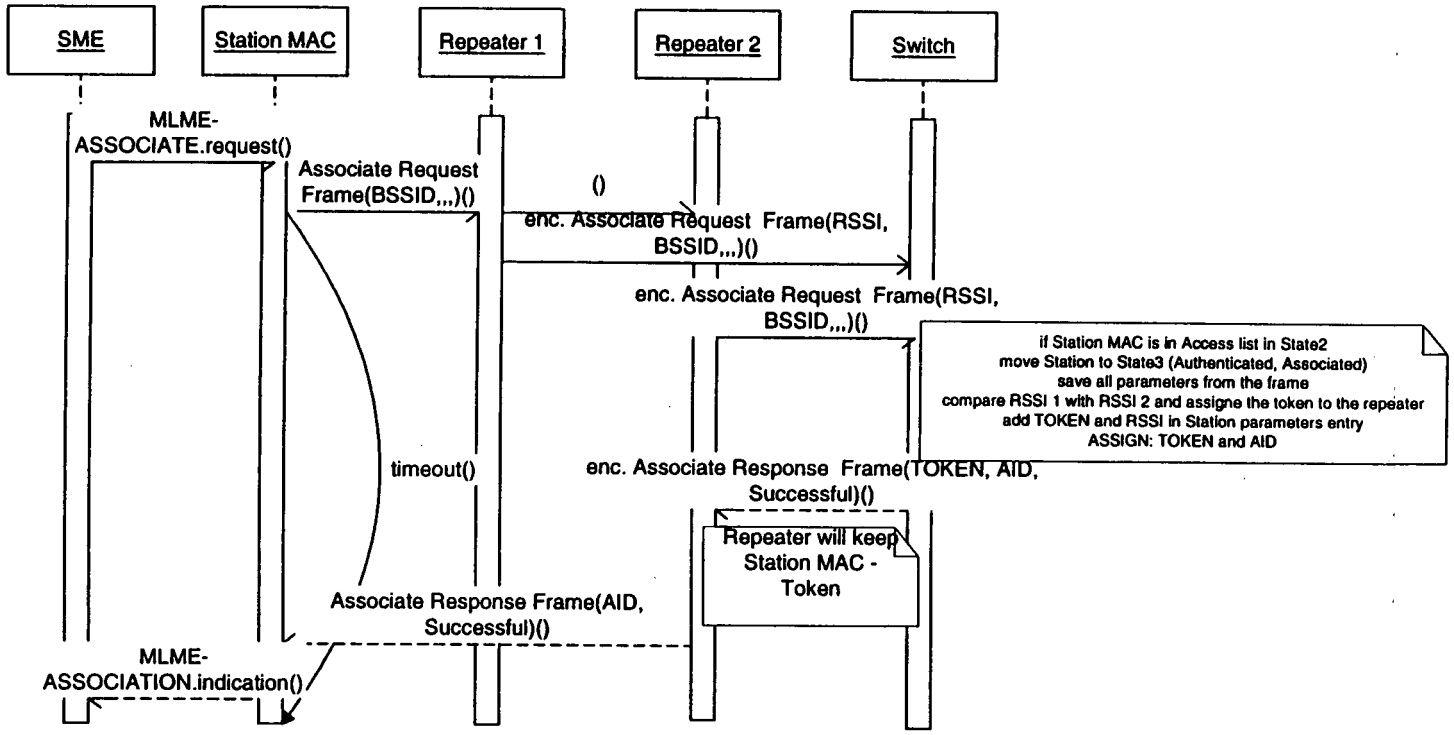

SME
Station MAC
Repeater 1
Repeater 2
Switch
MLME-
ASSOCIATE.request()
Associate Request
Frame(BSSID,,,)()
()
enc. Associate Request Frame(RSSI,
BSSID,,,)()
enc. Associate Request Frame(RSSI,
BSSID,,,)()
if Station MAC is in Access list in State2
move Station to State3 (Authenticated, Associated)
save all parameters from the frame
compare RSSI 1 with RSSI 2 and assigne the token to the repeater
add TOKEN and RSSI in Station parameters entry
ASSIGN: TOKEN and AID
timeout()
enc. Associate Response Frame(TOKEN, AID,
Successful)()
Repeater will keep
Station MAC -
Token
Associate Response Frame(AID,
Successful)()
MLME-
ASSOCIATION.indication()

FIG. 19

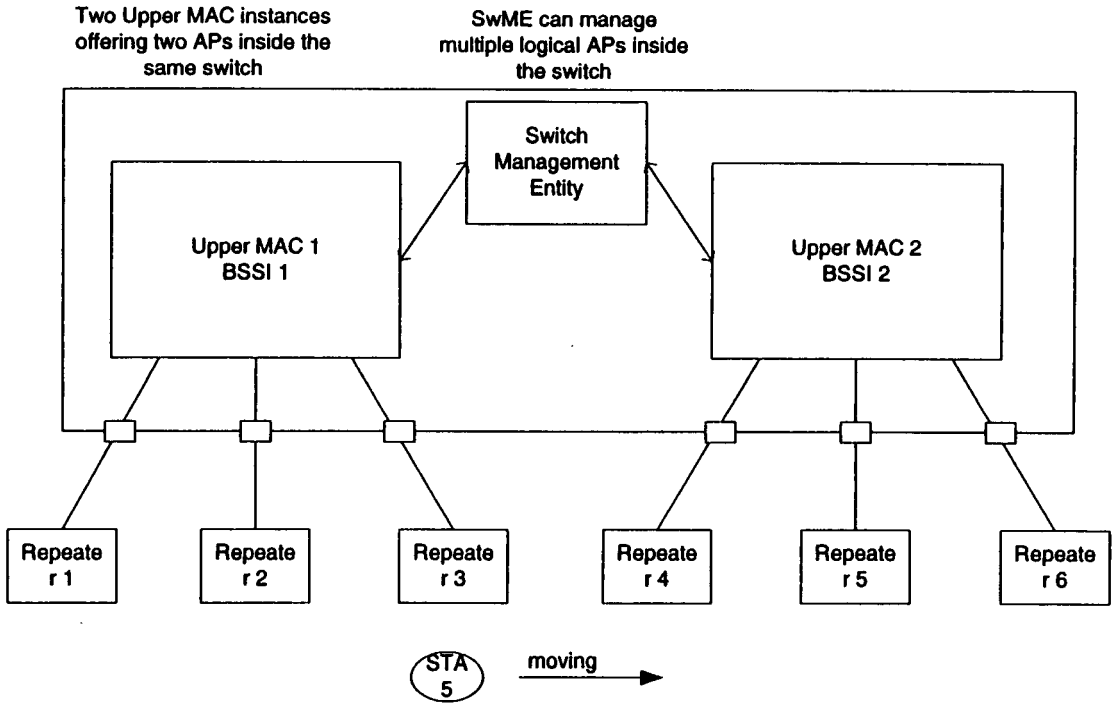

Two Upper MAC instances offering two APs inside the same switch
SwME can manage multiple logical APs inside the switch
Switch Management Entity
Upper MAC 1 BSSI 1
Upper MAC 2 BSSI 2
Repeate r 1
Repeate r 2
Repeate r 3
Repeate r 4
Repeate r 5
Repeate r 6
STA 5
moving

FIG. 20

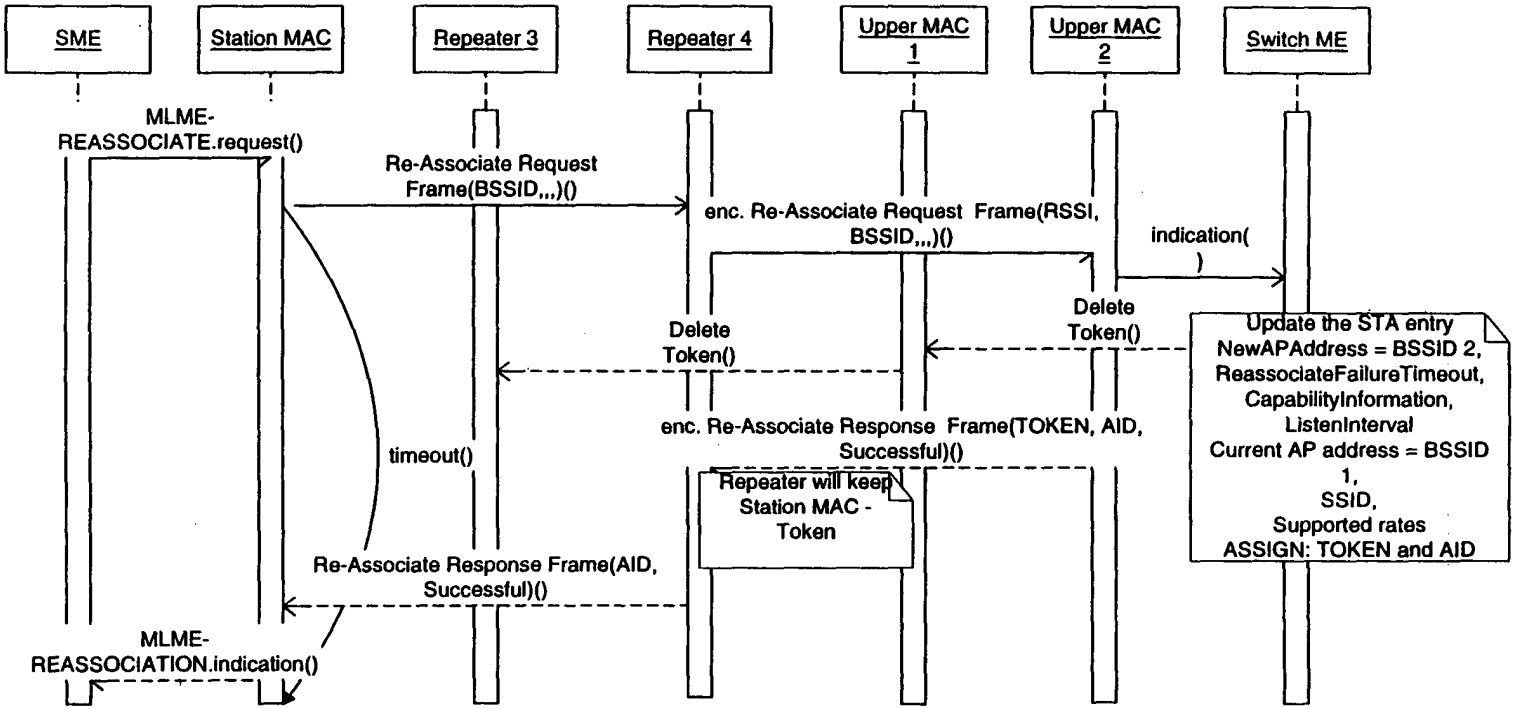

SME
Station MAC
Repeater 3
Repeater 4
Upper MAC 1
Upper MAC 2
Switch ME
MLME-REASSOCIATE.request()
Re-Associate Request Frame(BSSID,,,)()
enc. Re-Associate Request Frame(RSSI, BSSID,,,)()
indication( )
Delete Token()
Delete Token()
Update the STA entry
NewAPAddress = BSSID 2,
ReassociateFailureTimeout,
CapabilityInformation,
ListenInterval
Current AP address = BSSID 1,
SSID,
Supported rates
ASSIGN: TOKEN and AID
timeout()
enc. Re-Associate Response Frame(TOKEN, AID, Successful)()
Repeater will keep Station MAC - Token
Re-Associate Response Frame(AID, Successful)()
MLME-REASSOCIATION.indication()

FIG. 21

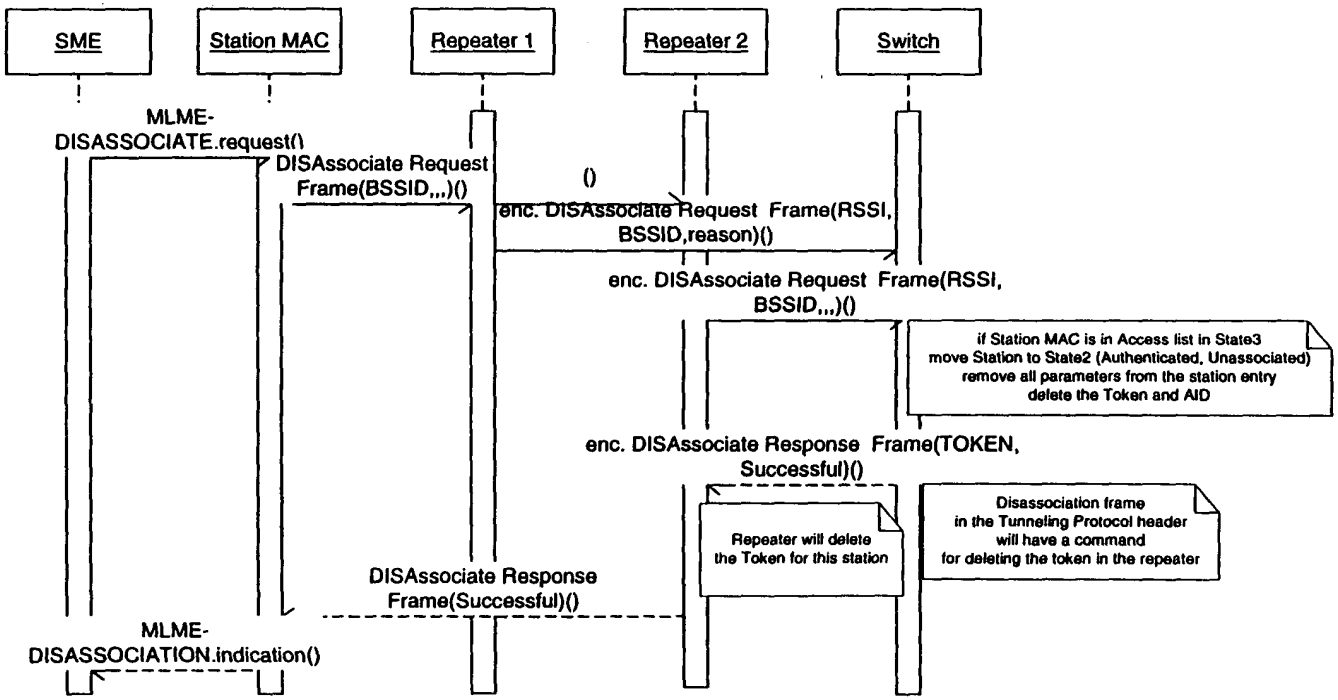

SME
Station MAC
Repeater 1
Repeater 2
Switch
MLME-
DISASSOCIATE.request()
DISAssociate Request
Frame(BSSID,,,)()
()
enc. DISAssociate Request Frame(RSSI,
BSSID,reason)()
enc. DISAssociate Request Frame(RSSI,
BSSID,,,)()
if Station MAC is in Access list in State3
move Station to State2 (Authenticated, Unassociated)
remove all parameters from the station entry
delete the Token and AID
enc. DISAssociate Response Frame(TOKEN,
Successful)()
Repeater will delete
the Token for this station
Disassociation frame
in the Tunneling Protocol header
will have a command
for deleting the token in the repeater
DISAssociate Response
Frame(Successful)()
MLME-
DISASSOCIATION.indication()

FIG. 22

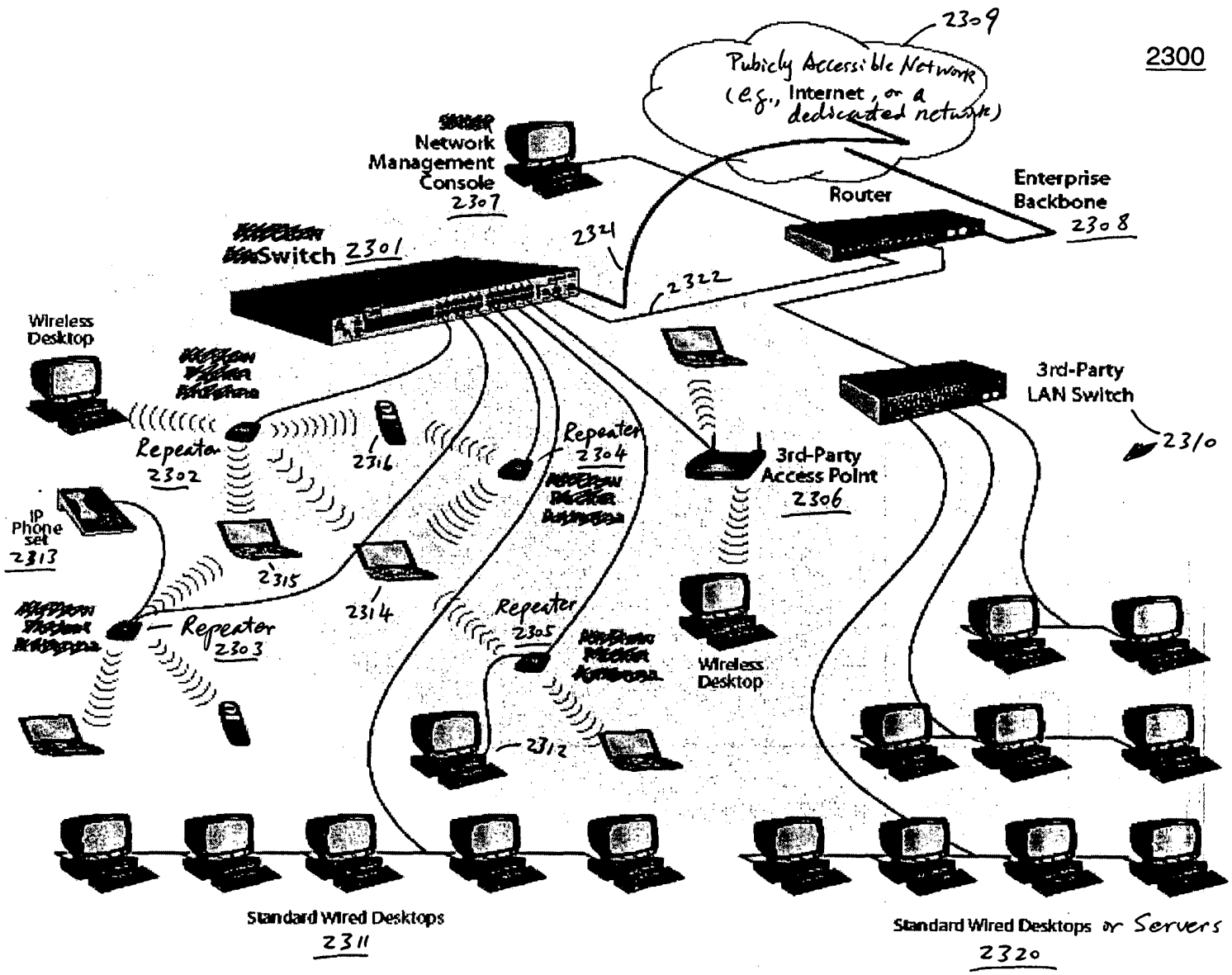

2309
Pubicly Accessible Network
(e.g., Internet, or a dedicated network)
2300
Network Management Console 2307
Router
Enterprise Backbone 2308
Switch 2301
2321
2322
Wireless Desktop
3rd-Party LAN Switch
2310
Repeater 2302
2316
Repeater 2304
3rd-Party Access Point 2306
IP Phone set 2313
2315
2314
Repeater 2303
Repeater 2305
Wireless Desktop
2312
Standard Wired Desktops 2311
Standard Wired Desktops or Servers 2320

Fig. 23

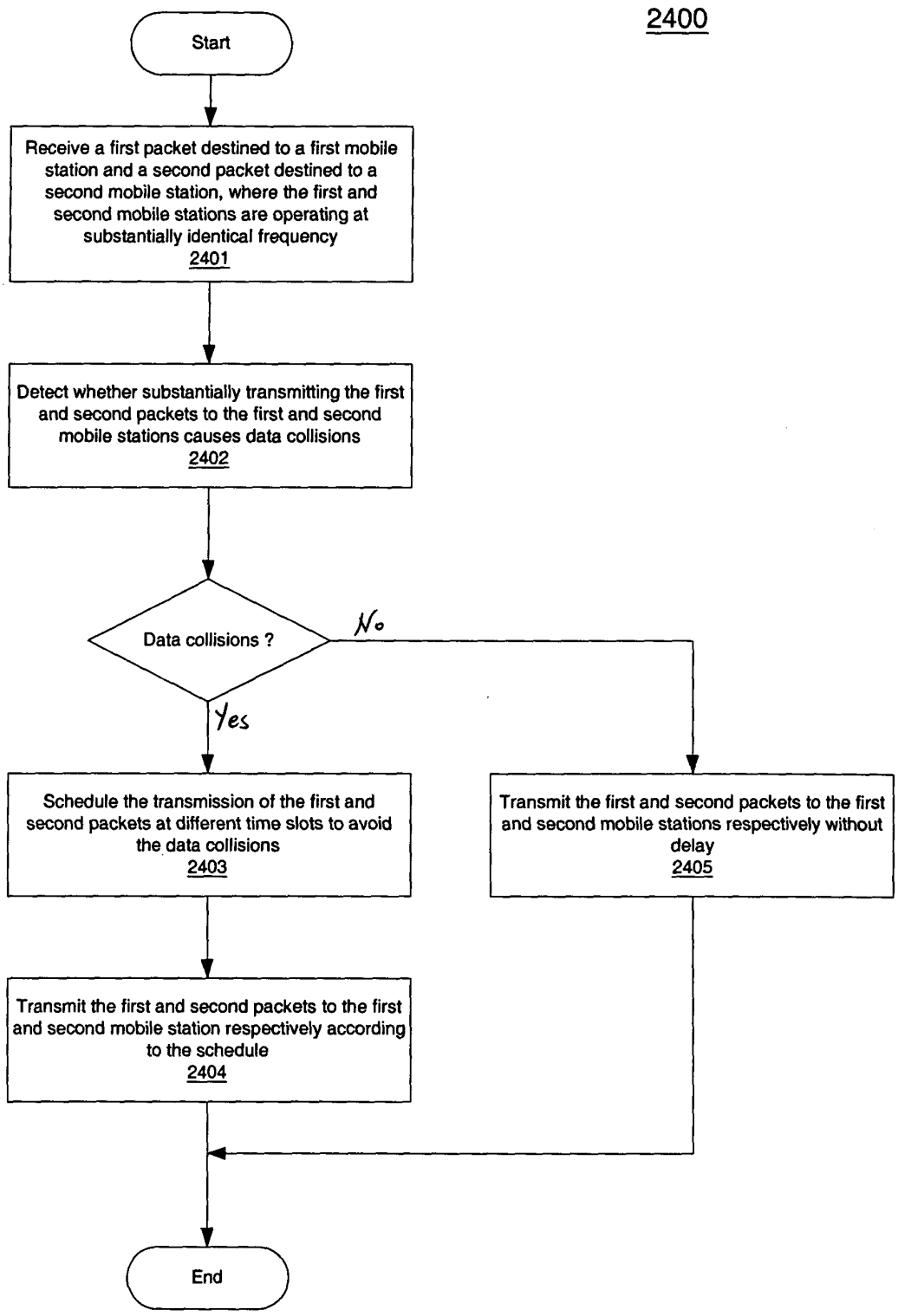

2400
Start
Receive a first packet destined to a first mobile station and a second packet destined to a second mobile station, where the first and second mobile stations are operating at substantially identical frequency
2401
Detect whether substantially transmitting the first and second packets to the first and second mobile stations causes data collisions
2402
Data collisions ?
No
Yes
Schedule the transmission of the first and second packets at different time slots to avoid the data collisions
2403
Transmit the first and second packets to the first and second mobile station respectively according to the schedule
2404
Transmit the first and second packets to the first and second mobile stations respectively without delay
2405
End

Fig. 24A

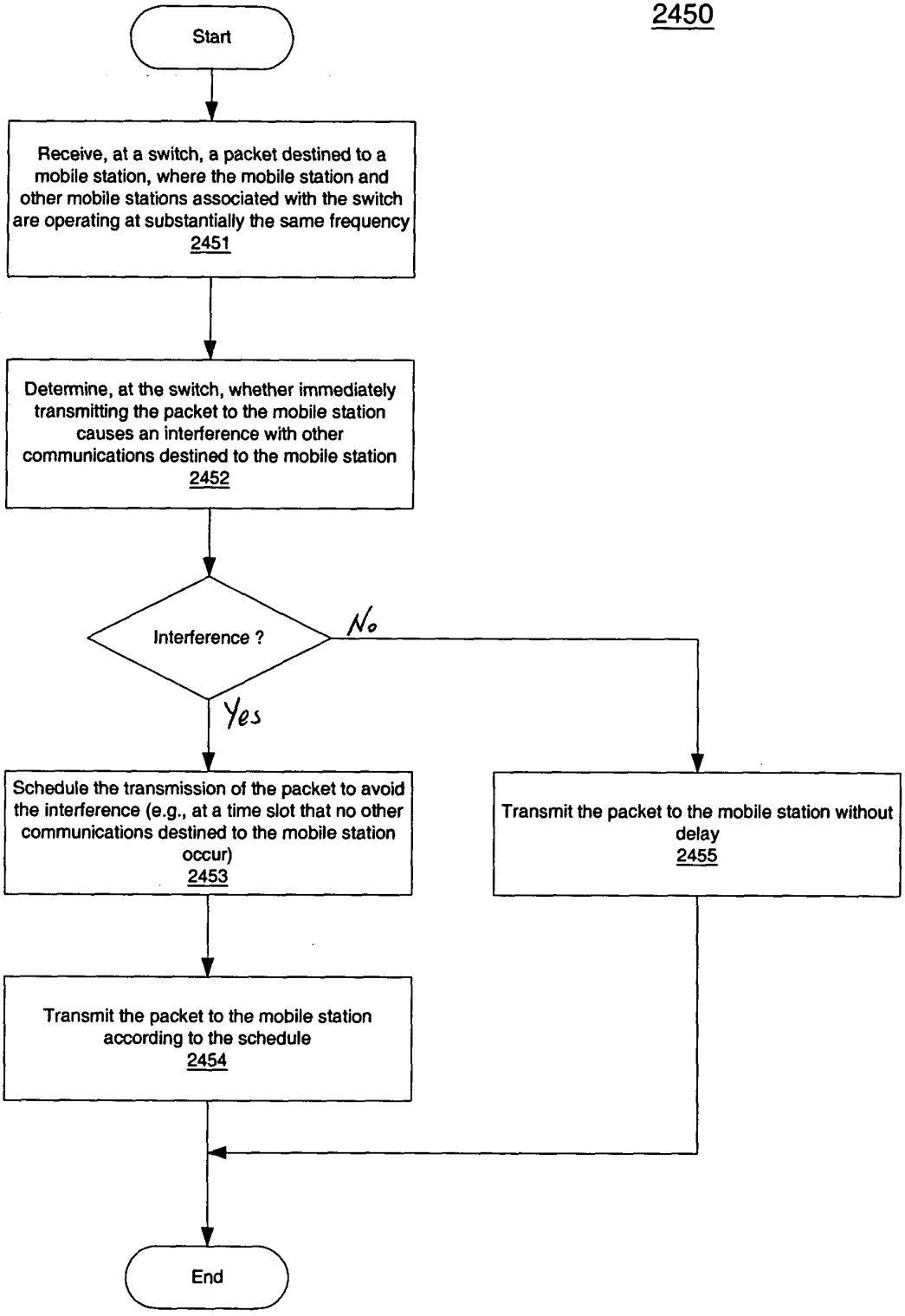

2450
Start
Receive, at a switch, a packet destined to a mobile station, where the mobile station and other mobile stations associated with the switch are operating at substantially the same frequency
2451
Determine, at the switch, whether immediately transmitting the packet to the mobile station causes an interference with other communications destined to the mobile station
2452
Interference ?
No
Yes
Schedule the transmission of the packet to avoid the interference (e.g., at a time slot that no other communications destined to the mobile station occur)
2453
Transmit the packet to the mobile station without delay
2455
Transmit the packet to the mobile station according to the schedule
2454
End

Fig. 24B

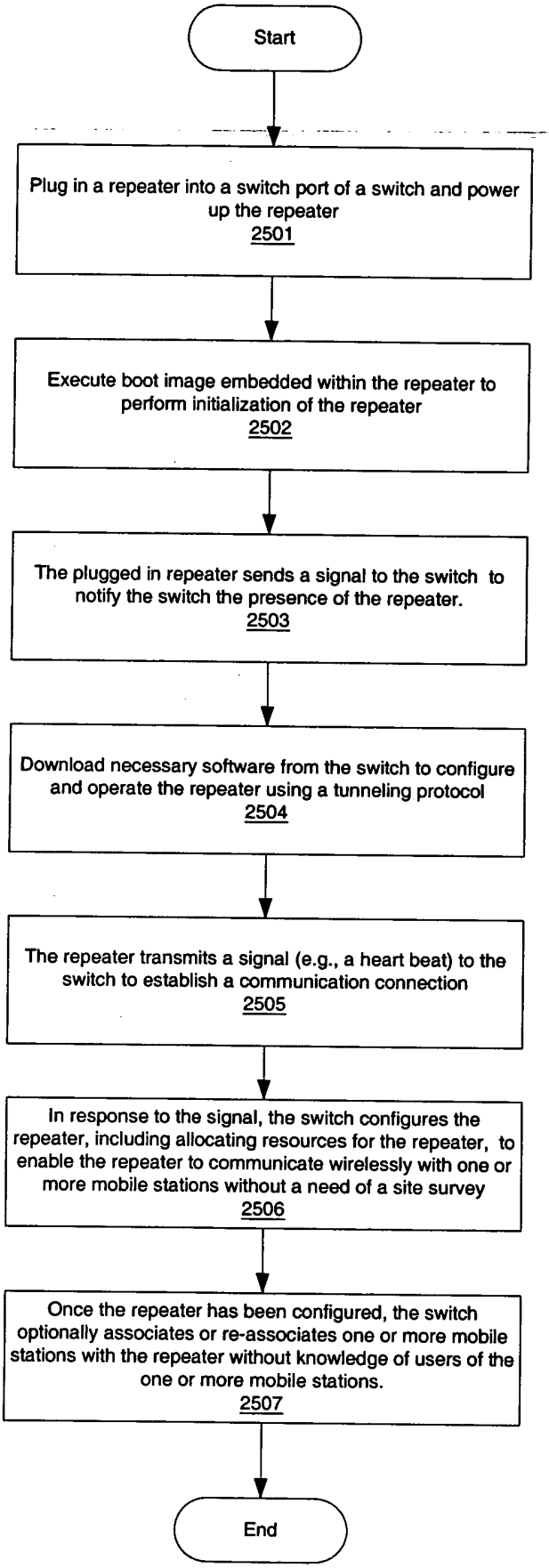

Start
2500
Plug in a repeater into a switch port of a switch and power up the repeater
2501
Execute boot image embedded within the repeater to perform initialization of the repeater
2502
The plugged in repeater sends a signal to the switch to notify the switch the presence of the repeater.
2503
Download necessary software from the switch to configure and operate the repeater using a tunneling protocol
2504
The repeater transmits a signal (e.g., a heart beat) to the switch to establish a communication connection
2505
In response to the signal, the switch configures the repeater, including allocating resources for the repeater, to enable the repeater to communicate wirelessly with one or more mobile stations without a need of a site survey
2506
Once the repeater has been configured, the switch optionally associates or re-associates one or more mobile stations with the repeater without knowledge of users of the one or more mobile stations.
2507
End

Fig. 25A

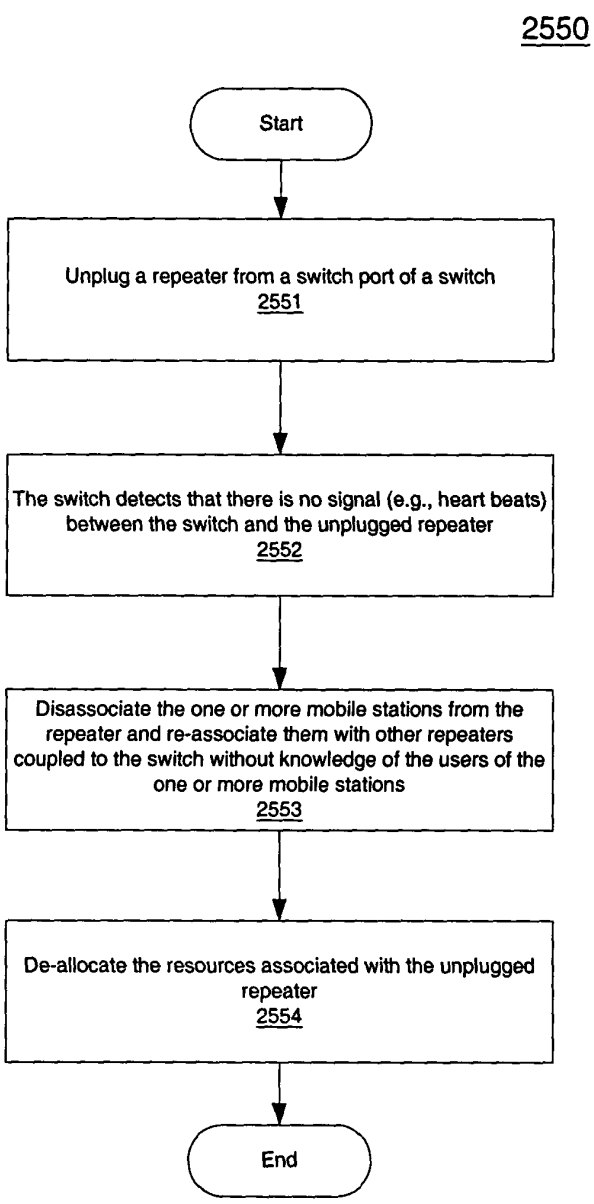

2550
Start
Unplug a repeater from a switch port of a switch
2551
The switch detects that there is no signal (e.g., heart beats) between the switch and the unplugged repeater
2552
Disassociate the one or more mobile stations from the repeater and re-associate them with other repeaters coupled to the switch without knowledge of the users of the one or more mobile stations
2553
De-allocate the resources associated with the unplugged repeater
2554
End

Fig. 25B

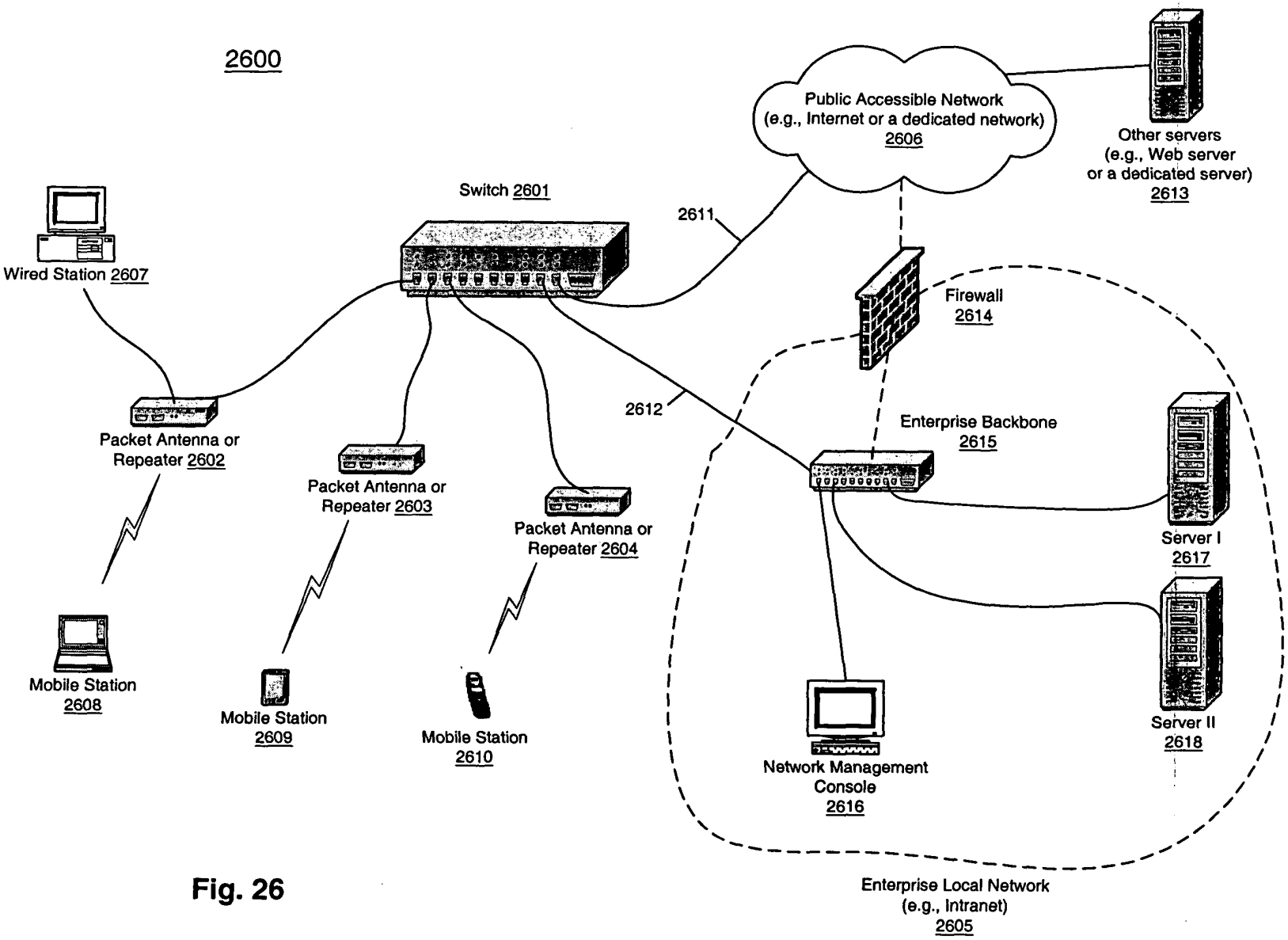

2600
Public Accessible Network
(e.g., Internet or a dedicated network)
2606
Other servers
(e.g., Web server
or a dedicated server)
2613
Switch 2601
2611
Wired Station 2607
Firewall
2614
Packet Antenna or
Repeater 2602
2612
Enterprise Backbone
2615
Packet Antenna or
Repeater 2603
Packet Antenna or
Repeater 2604
Server I
2617
Mobile Station
2608
Mobile Station
2609
Mobile Station
2610
Server II
2618
Network Management
Console
2616
Enterprise Local Network
(e.g., Intranet)
2605

Fig. 26

2700

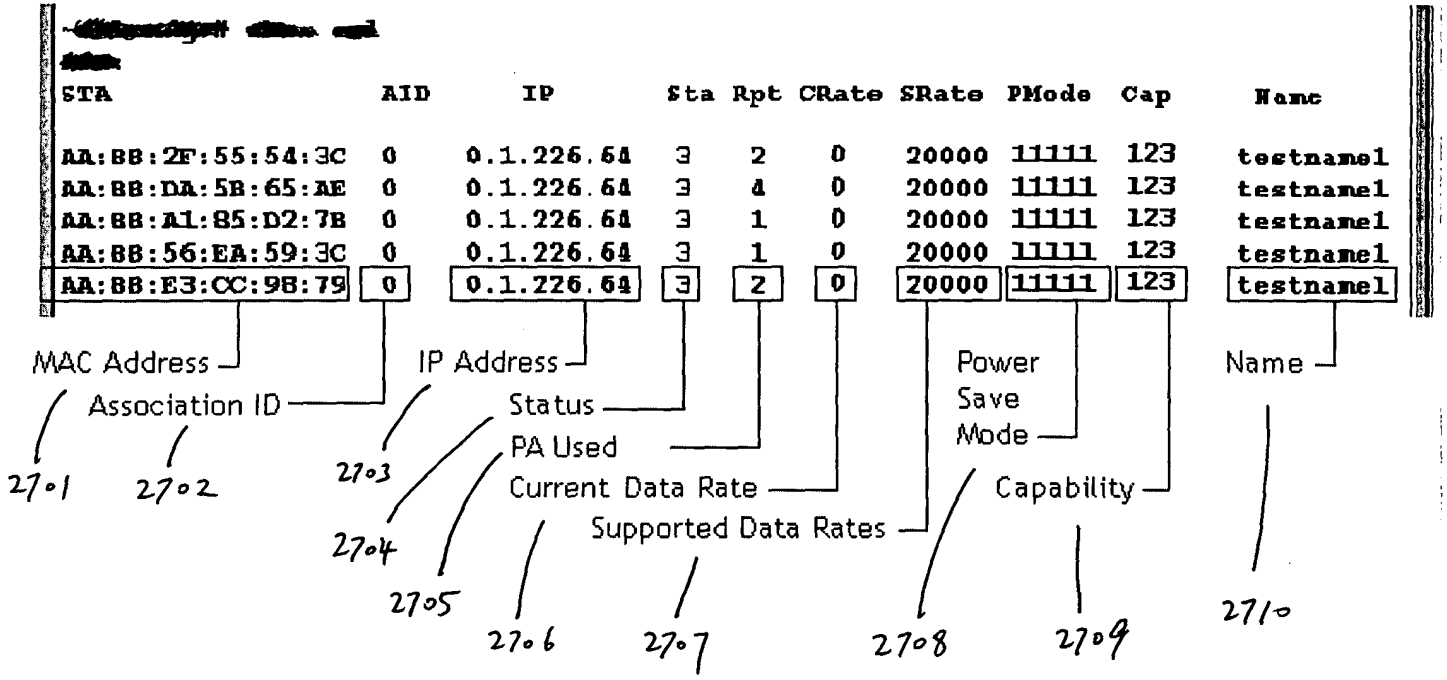

STA
AID
IP
Sta
Rpt
CRate
SRate
PMode
Cap
Name
AA:BB:2F:55:54:3C 0 0.1.226.64 3 2 0 20000 11111 123 testname1
AA:BB:DA:5B:65:AE 0 0.1.226.64 3 4 0 20000 11111 123 testname1
AA:BB:A1:85:D2:7B 0 0.1.226.64 3 1 0 20000 11111 123 testname1
AA:BB:56:EA:59:3C 0 0.1.226.64 3 1 0 20000 11111 123 testname1
AA:BB:E3:CC:9B:79 0 0.1.226.64 3 2 0 20000 11111 123 testname1
MAC Address
Association ID
IP Address
Status
PA Used
Current Data Rate
Supported Data Rates
Power Save Mode
Capability
Name
2701
2702
2703
2704
2705
2706
2707
2708
2709
2710

Fig. 27

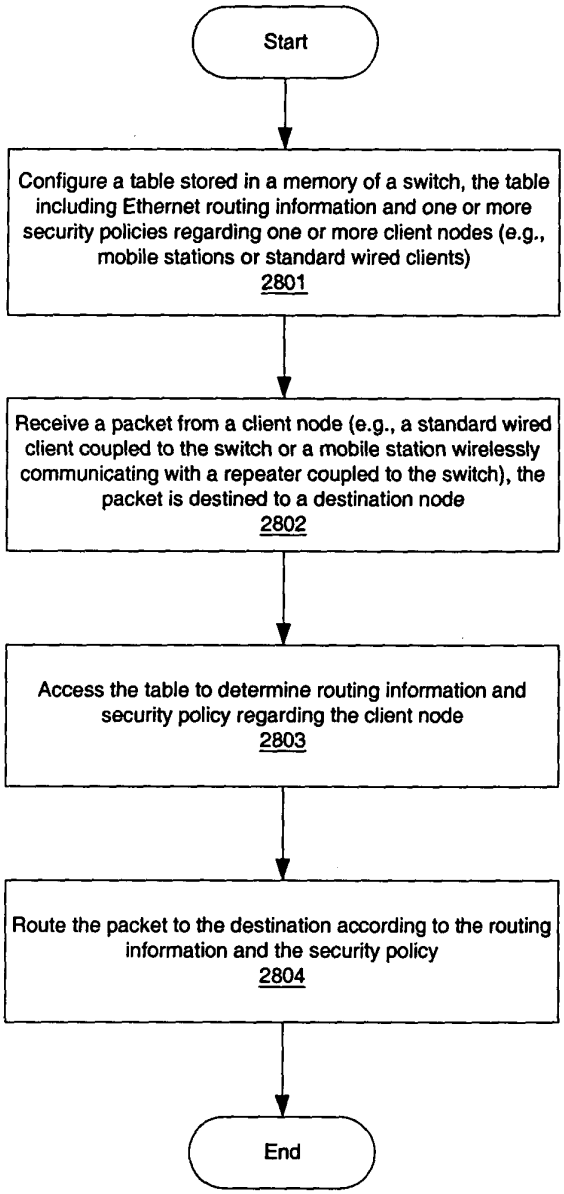

Start
2800
Configure a table stored in a memory of a switch, the table including Ethernet routing information and one or more security policies regarding one or more client nodes (e.g., mobile stations or standard wired clients)
2801
Receive a packet from a client node (e.g., a standard wired client coupled to the switch or a mobile station wirelessly communicating with a repeater coupled to the switch), the packet is destined to a destination node
2802
Access the table to determine routing information and security policy regarding the client node
2803
Route the packet to the destination according to the routing information and the security policy
2804
End

Fig. 28

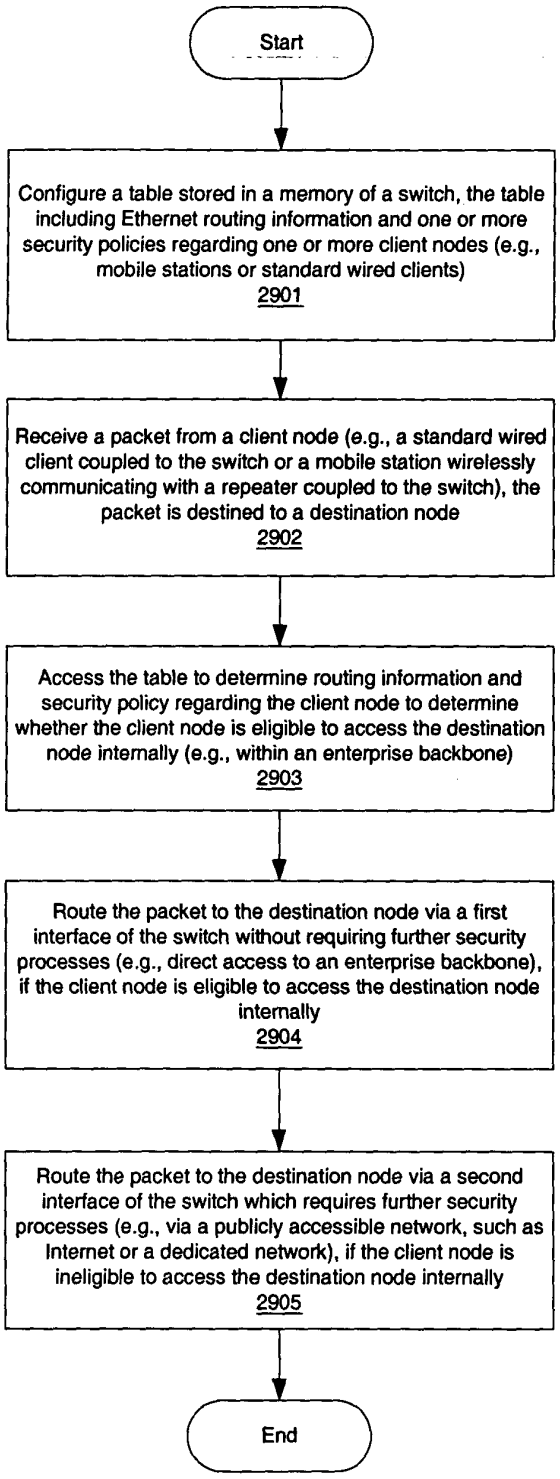

Start
2900
Configure a table stored in a memory of a switch, the table including Ethernet routing information and one or more security policies regarding one or more client nodes (e.g., mobile stations or standard wired clients)
2901
Receive a packet from a client node (e.g., a standard wired client coupled to the switch or a mobile station wirelessly communicating with a repeater coupled to the switch), the packet is destined to a destination node
2902
Access the table to determine routing information and security policy regarding the client node to determine whether the client node is eligible to access the destination node internally (e.g., within an enterprise backbone)
2903
Route the packet to the destination node via a first interface of the switch without requiring further security processes (e.g., direct access to an enterprise backbone), if the client node is eligible to access the destination node internally
2904
Route the packet to the destination node via a second interface of the switch which requires further security processes (e.g., via a publicly accessible network, such as Internet or a dedicated network), if the client node is ineligible to access the destination node internally
2905
End

Fig. 29

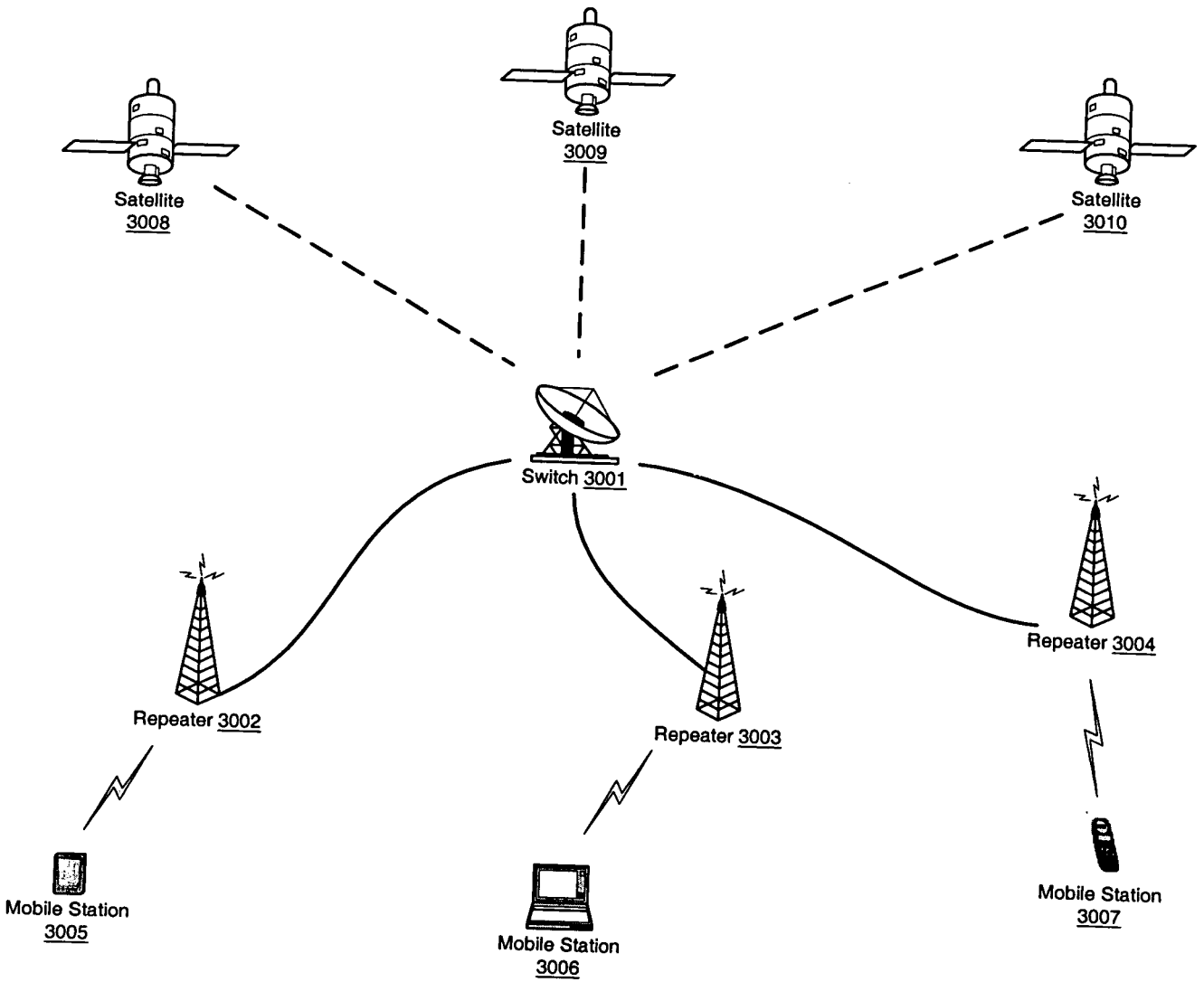

3000
Satellite
3009
Satellite
3008
Satellite
3010
Switch 3001
Repeater 3002
Repeater 3003
Repeater 3004
Mobile Station
3005
Mobile Station
3006
Mobile Station
3007

Fig. 30